Défense nationale / National Defence

B-GL-300-005/FP-002

FORCE TERRESTRE
OPÉRATIONS D'INFORMATION
(FRANÇAIS)

AVERTISSEMENT

QUOIQUE CETTE PUBLICATION NE PORTE PAS DE CLASSIFICATION DE SÉCURITÉ ON PEUT EN RESTREINDRE L'ACCÈS AU PUBLIC EN TOUT OU EN PARTIE SELON LA LOI SUR L'ACCÈS À L'INFORMATION. LES INFORMATIONS QUI Y SONT CONTENUES DOIVENT ÊTRE EXAMINÉES EN DÉTAIL POUR DÉTERMINER SI LA TOTALITÉ OU UNE PARTIE DE CETTE PUBLICATION PEUT ÊTRE DIVULGUÉE AU PUBLIC.

(La présente publication prend effet dès sa réception.)

Publié avec l'autorisation du Chef d'état-major de la Défense

BPR : DDAT 5

1999-01-18

Canada

AVANT-PROPOS

1. La B-GL-300-005/FP-002, *Opérations d'information*, est publiée avec l'autorisation du Chef d'état-major de la Défense.

2. La présente publication prend effet dès sa réception.

3. Toute proposition de modification possible doit être transmise par la voie hiérarchique au directeur de la Doctrine de l'Armée de terre, attention DDAT 5, Fort Fontenac, BP 17000, Succ Forces, Kingston, ON, K7K 7B4.

4. À moins d'indication contraire, les pronoms masculins s'appliquent tant aux hommes qu'aux femmes.

5. L'IDDN de la version anglaise de la présente publication est B-GL-300-005/FP-001. La terminologie utilisée dans cette publication est conforme au vocabulaire de l'Armée de terre.

104-03705/

PRÉFACE

GÉNÉRALITÉS

1. Le présent manuel de doctrine décrit un concept multidimensionnel utilisé par l'Armée de terre pour assurer le succès de l'ensemble des opérations. L'Armée de terre a fait des Opérations d'information (OI) une fonction de combat essentielle qu'il convient d'intégrer aux autres fonctions de combat pour maximiser la puissance de combat. Les composants des OI ne sont pas nouveaux, certains sont utilisés dans la conduite de la guerre depuis des milliers d'années. Ce qui est nouveau, c'est l'emphase placée sur l'intégration de ces composants dans un but de maximisation de la puissance de combat. Le but des OI est la supériorité de l'information par l'exploitation optimale de l'information et le refus de la même possibilité à l'adversaire.

BUT

2. La publication B-GL-300-005/FP-002, *Opérations d'information* vise à décrire le concept en détail, et à donner un aperçu de la façon dont les OI sont reliées aux autres fonctions de combat et contribuent au succès sur le champ de bataille.

PORTÉE

3. Le cœur de ce concept est l'idée qu'il existe deux environnements d'information, à savoir l'environnement global de l'information (EGI) et l'environnement militaire de l'information (EMI). Ces environnements regroupent dans un contexte civil et militaire toutes les agences et procédures, ainsi que tous les groupes, individus et systèmes, reliés à l'information. Cette activité opérationnelle est dynamique et complexe, et exige beaucoup de coordination. Elle réunit de nombreuses disciplines traditionnellement séparées et des technologies nouvelles de manière à fournir au commandant la supériorité de l'information nécessaire au succès.

4. L'Armée de terre a structuré cette fonction de combat en six éléments regroupés comme suit :

a. Quatre éléments de soutien :

(1) les systèmes d'information et de communication (SIC),

(2) l'information pertinente, y compris le renseignement, la surveillance, l'acquisition des objectifs et la reconnaissance (système ISTAR),

(3) la coopération civilo-militaire (COCIM);

(4) les affaires publiques (AP).

b. deux éléments d'action :

(1) les Opérations d'information offensives (OI off);

(2) les Opérations d'information défensives (OI déf).

5. Les OI, en tant que fonction de combat, englobent une dimension humaine, morale, physique et électromagnétique. La doctrine et les principes définis dans la présente publication s'appliquent aux niveaux opérationnel et tactique de commandement dans l'éventail complet des types de conflits possibles.
La doctrine des OI de niveau stratégique est contenue dans la B-GG-005-004/AF-032, *Opérations d'information des Forces canadiennes.*

TABLE DES MATIÈRES

AVANT-PROPOS i

PRÉFACE iii

Généralités iii

But iii

Portée iii

CHAPITRE 1 OPÉRATIONS D'INFORMATION ET ENVIRONNEMENT OPÉRATIONNEL

SECTION 1 INTRODUCTION 1

SECTION 2 CONCEPT D'OPÉRATIONS D'INFORMATION 2

SECTION 3 ENVIRONNEMENT OPÉRATIONNEL 5

SECTION 4 TECHNOLOGIE 8

SECTION 5 GESTION DE L'INFORMATION 14

CHAPITRE 2 PRINCIPES DE BASE, ÉLÉMENTS ET ACTIVITÉS

SECTION 1 INTRODUCTION 17

SECTION 2 PRINCIPES DE BASE 17

SECTION 3 ÉLÉMENTS 18

Systèmes d'information et de communication 19

Architecture 19

Intégration 20

Connectivité globale 20

Gestion de l'information 21

Information pertinente 22

Affaires publiques 24

Coopération civilo-militaire 26

Opérations d'information offensives et défensives 26

Opérations d'information offensives 27

Opérations d'information défensives 27

SECTION 4 ACTIVITÉS 28

Acquérir 28

Utiliser 29

Vérifier 31

Gérer 32

Protéger 33

Empêcher 34

SECTION 5 INTERACTION AVEC D'AUTRES FONCTIONS DE COMBAT 35

Commandement 35

Protection 36

Puissance de feu 36

Manoeuvre 37

Maintien en puissance 37

CHAPITRE 3 SYSTÈMES D'INFORMATION ET DE COMMUNICATION

SECTION 1 L'ENVIRONNEMENT 39

SECTION 2 FONCTIONS 40

SECTION 3 RÔLE 42

SECTION 4 SYSTÈMES MILITAIRES 43

SECTION 5 SYSTÈMES D'INFORMATION NON MILITAIRES 45

SECTION 6 PLANIFICATION DES COMMUNICATIONS ET DES SYSTÈMES D'INFORMATION 47

Systèmes d'information non militaires 47

Instruction 47

Soutien des communications 47

Capacités 48

Technologie future 49

Sécurité 49

Gestion des systèmes d'information et de communications .. 50

CHAPITRE 4 INFORMATION PERTINENTE

SECTION 1 INTRODUCTION 53

SECTION 2 INFORMATION PERTINENTE 53

SECTION 3 CRITÈRES D'ÉVALUATION 55

SECTION 4 RENSEIGNEMENT 56

Rôle du renseignement 57

Fonctions de renseignement 58

Évaluation des points vulnérables des forces amies – contre-ingérence 58

Compréhension de l'adversaire 59

SECTION 5 UTILISATION DE L'ANALYSE TACTIQUE GRAPHIQUE 59

SECTION 6 ÉVALUATION DES DOMMAGES AU COMBAT 61

CHAPITRE 5 RENSEIGNEMENT, SURVEILLANCE, ACQUISITION D'OBJECTIF ET RECONNAISSANCE DANS LES OPÉRATIONS TERRESTRES

SECTION 1 INTRODUCTION 63

SECTION 2 LE CONCEPT DU SYSTÈME ISTAR 64

SECTION 3 LES PRINCIPES DU SYSTÈME ISTAR 65

SECTION 4 LES ACTIVITÉS DU SYSTÈME ISTAR 66

SECTION 5 SOURCES ET ORGANISMES 68

SECTION 6 PLANIFICATION ET EXÉCUTION DU PROCESSUS D'ISTAR 70

SECTION 7 LE PROCESSUS DE CHOIX DES OBJECTIFS 71

CHAPITRE 6 OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES

SECTION 1 INTRODUCTION 75

Rôle des opérations d'information offensives et défensives 76

SECTION 2 ÉLÉMENTS 77

Information pertinente 77

Systèmes d'information et de communications 78

Sécurité des opérations 78

Contre-ingérence 79

Déception militaire 79

Opérations psychologiques 80

Contre-OPSPSY 81

Guerre électronique 81

Attaque des réseaux d'ordinateurs 83

Opérations d'information spéciales 83

Destruction matérielle 84

SECTION 3 OPÉRATIONS D'INFORMATION OFFENSIVES 85

SECTION 4 OPÉRATIONS D'INFORMATION DÉFENSIVES 88

SECTION 5 COORDINATION 91

CHAPITRE 7 AFFAIRES PUBLIQUES

SECTION 1 INTRODUCTION 93

SECTION 2 ENVIRONNEMENT DE L'INFORMATION 94

SECTION 3 RÔLE DES AFFAIRES PUBLIQUES DANS LE SOUTIEN DES OPÉRATIONS D'INFORMATION 95

SECTION 4 CONSIDÉRATIONS EN MATIÈRE DE PLANIFICATION DES AFFAIRES PUBLIQUES 100

SECTION 5 COMMANDEMENT ET CONTRÔLE DES AFFAIRES PUBLIQUES 101

CHAPITRE 8 COOPÉRATION CIVILO-MILITAIRE

SECTION 1 INTRODUCTION ET DÉFINITIONS 105

SECTION 2 OBJECTIFS DE L'ARMÉE DE TERRE EN MATIÈRE DE COOPÉRATION CIVILO-MILITAIRE 107

SECTION 3 TYPES DE COOPÉRATION CIVILO-MILITAIRE 109

SECTION 4 LIENS ENTRE LA COOPÉRATION CIVILO-MILITAIRE, LES OPÉRATIONS PSYCHOLOGIQUES ET LES AFFAIRES PUBLIQUES 110

SECTION 5 SOURCES D'INFORMATION 111

SECTION 6 COCIM ET INFORMATION 113

SECTION 7 LIMITATIONS / ACTIVITÉS NON AUTORISÉES 114

ANNEXE A SOUTIEN MUTUEL DES ÉLÉMENTS DES OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES 115

TABLE DES FIGURES

Figure 1-2-1 : Cycle de décision-action du commandant 3

Figure 1-3-2 : La zone d'opérations multidimensionnelle 7

Figure 1-4-3 : Avantages de la fusion des données et de l'information 10

Figure 1-4-4 : Secteurs technologiques clés du point de vue de la visualisation du champ de bataille 11

Figure 1-4-5 : La hiérarchie cognitive et l'art des opérations 13

Figure 2-3-1 : Environnement global de l'information 18

Figure 2-4-2 : Activités d'opérations d'information 28

Figure 3-1-1 : Vitesse croissante du flux et du traitement de l'information au cours des âges 40

Figure 3-3-2 : Réseau de communications globales 43

Figure 3-4-3 : Systèmes d'information et de communication de la Force terrestre 45

Figure 4-2-1 : Information pertinente 54

Figure 8-1-1 : COCIM et le spectre des conflits 107

Figure 8-2-2 : L'environnement opérationnel 109

Figure 8-3-3 : Types de coopération civilo-militaire 110

CHAPITRE 1
OPÉRATIONS D'INFORMATION ET ENVIRONNEMENT OPÉRATIONNEL

La victoire sourit à ceux qui anticipent les changements dans le caractère de la guerre, et non à ceux qui s'adaptent après que les changements se sont produits. [1]

Général Gulio Douhet (1869-1930)

SECTION 1
INTRODUCTION

1. Le présent chapitre vise à introduire le concept d'Opérations d'information (OI), et à décrire l'environnement et la technologie des OI. Un certain nombre de tendances ont des répercussions importantes sur le champ de bataille, dont l'application asymétrique de la puissance de combat, la nature de plus en plus non linéaire et non contiguë du champ de bataille, et l'importance croissante des concepts et technologies de la *« guerre de l'âge de l'information »*[2]. Nombre d'ouvrages et d'articles ont été écrits sur ces sujets. Tous décrivent la dépendance croissante des armées modernes vis-à-vis de l'information et l'augmentation considérable de la quantité d'information aujourd'hui. Ceci n'inclut pas seulement la quantité d'information pertinente, mais également sa nature, sa complexité, la possibilité d'y avoir accès, la dépendance croissante envers cette information, la rapidité avec laquelle elle est obtenue et enfin, la technologie qui en fait l'acquisition, le traitement, la distribution et le stockage.

---

[1] Le général Giulio Douhet est souvent cité par les historiens militaires comme le Clausewitz de la stratégie aérienne. Officier de l'artillerie italienne avant la Première guerre mondiale, il a obtenu le commandement de la première unité aérienne de l'armée italienne et effectué des bombardements aériens en Libye pendant la guerre italo-turque de 1911–1912. Ses idées ambitieuses sur la stratégie aérienne, exposées dans son ouvrage intitulé *Le commandement des airs (Il Dominio dell'aria)* reconnaissaient dès 1915 que l'avion était une arme de puissance offensive illimitée.

[2] Alvin et Heidi Toffler, Guerre et contre-guerre: *La troisième vague*, Morrow, New York, 1980.

2. Les OI sont un élément essentiel de la puissance de combat qui permet aux commandants d'accomplir leur mission dans le cadre de l'approche manœuvriste à l'âge de l'information.

3. Les OI ne sont pas nouvelles. Dans leur forme la plus simple, elles englobent l'ensemble des opérations d'acquisition de l'information et des connaissances qui améliorent l'exécution des opérations amies tout en refusant des avantages similaires à l'ennemi par tous les moyens possibles.

4. L'intégration appropriée des OI aide nos forces à prendre l'initiative, et à demeurer physiquement et mentalement plus agiles que l'ennemi aux moments et lieux propices, et avec les armes et ressources appropriées.

SECTION 2
CONCEPT D'OPÉRATIONS D'INFORMATION

5. Le principal objectif des OI est d'assurer la supériorité et l'avantage relatif du cycle de décision-action du commandant ami (voir la figure 1-2-1) par rapport à celui de l'adversaire, et d'utiliser cet avantage pour améliorer et faciliter l'utilisation d'autres éléments de la puissance de combat. Comme on peut le voir à la figure 1-1, l'application des OI peut améliorer la visualisation du champ de bataille, la définition de l'effort principal, la maîtrise du rythme des opérations et la synchronisation.

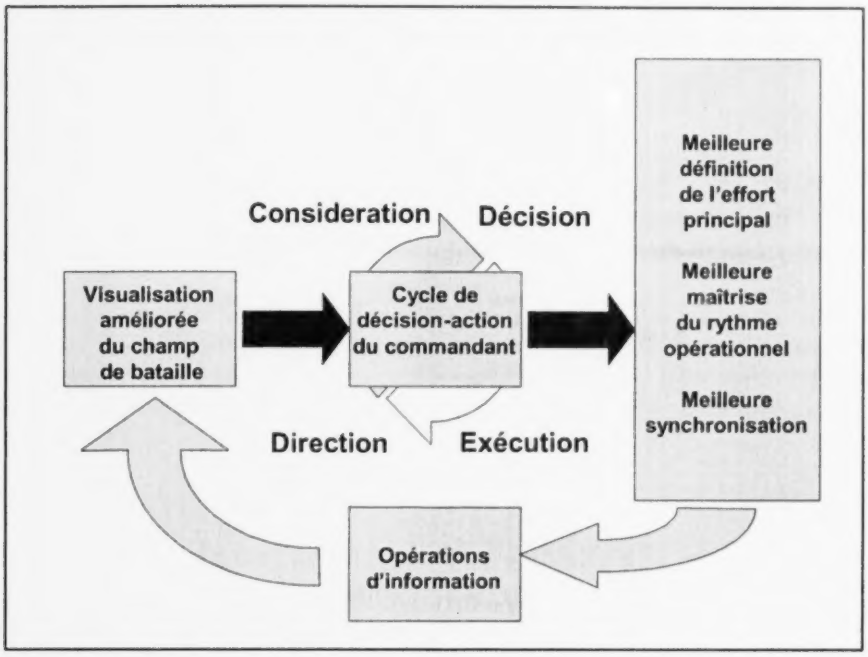

Figure 1-2-1 : Cycle de décision-action du commandant

6. L'état idéal des opérations est celui dans lequel nous possédons la domination de l'information. Une domination absolue et soutenue de l'environnement informationnel en expansion n'est pas possible. Les commandants visent en conséquence à réaliser la supériorité de l'information au bon endroit, au bon moment et dans les bonnes circonstances. La supériorité de l'information est la disparité qui existe entre ce que les forces amies savent de leur propre zone d'opérations et des opérations qui s'y déroulent, et ce que l'ennemi en sait.

7. La nature combative des OI signifie que la supériorité de l'information n'est ni continue ni assurée. Les commandants de l'Armée de terre visent la supériorité soutenue de l'information dans leur zone d'opérations. Dans certains cas, en particulier au début d'une opération, ils doivent se contenter d'une supériorité locale ou temporaire à des points de jonction critiques de leur opération. Même dans le cas d'une supériorité générale de l'information, les forces ennemies peuvent disposer de capacités supérieures à celles des forces amies sur certains aspects. Les commandants s'efforcent d'éviter les situations dans lesquelles les forces amies engagent le combat dans des conditions tactiques de parité ou d'infériorité de l'information. La supériorité de l'information n'est cependant pas une panacée; les commandants doivent

quand même prendre des risques, et n'ont pas le luxe d'attendre l'information et la formulation d'un plan parfaits.

8. Le cœur de ce concept est la notion qu'il existe un univers de l'information qui englobe tous les aspects de notre société et s'étend à tous les niveaux de l'action militaire, de la stratégie d'ensemble au niveau tactique le plus bas. Dans le but de créer un certain ordre dans cet univers, nous avons subdivisé ce dernier en deux environnements distincts, l'environnement global de l'information (EGI) et l'environnement militaire de l'information (EMI) (voir la figure 2-1). Ces environnements réunissent dans un contexte civil et militaire la totalité des agences, procédures, groupes, individus et systèmes qui ont trait à l'information. Le présent manuel portera sur l'EMI. Dans ce contexte, les OI rassemblent de nombreuses disciplines traditionnellement séparées et de nouvelles technologies pour fournir au commandant la supériorité de l'information et le potentiel qui lui permettront d'atteindre au succès.

9. Le but des OI est d'améliorer ou d'amplifier l'effet de la puissance de combat amie, et de diminuer celle de l'ennemi. Une fonction clé des OI consiste à paralyser, désorganiser ou diminuer la capacité de l'ennemi à appliquer ses systèmes d'OI. Les OI peuvent être offensives ou défensives. La Doctrine de l'Armée de terre a structuré cette fonction de combat en six éléments regroupés comme suit :

a. Quatre éléments de soutien :

   (1) les systèmes d'information et de communication (SIC),

   (2) l'information pertinente, y compris le renseignement, la surveillance, l'acquisition d'objectifs et la reconnaissance (système ISTAR),

   (3) la coopération civilo-militaire (COCIM),

   (4) les affaires publiques (AP);

b. Deux éléments d'action :

   (1) les Opérations d'information offensives (OI off),

   (2) les Opérations d'information défensives (OI déf).

10. Le plus souvent, les objectifs d'OI seront intégrés verticalement de manière à soutenir et tirer parti des possibilités supérieures des quartiers généraux. Ces objectifs peuvent être établis à un niveau aussi élevé que le gouvernement, et intégrés verticalement par l'entremise des commandants subordonnés. Les OI doivent également être intégrées horizontalement. Elles doivent être synchronisées avec les autres fonctions de combat de manière à maximiser la puissance de combat. La planification et l'exécution des OI ne sont pas effectuées dans l'isolation, et sont en conséquence intégrées à la B-GL-331-001/FP-001, *Doctrine de soutien du commandement*.

11. Les OI incluent également l'exploitation des moyens tactiques de l'Armée de terre. Cela implique non seulement la collecte de l'information, qui doit encore être analysée pour être utile, mais également le partage de cette information avec les unités supérieures, subordonnées et adjacentes afin que toutes opèrent à partir d'une image pertinente commune. Ce partage de l'information inclut également les forces interarmées et combinées, de même que les organisations gouvernementales, les organisations non gouvernementales (ONG) et les organisations supranationales comme l'Organisation des Nations Unies (ONU) ou l'Organisation des États américains (OÉA).

SECTION 3
ENVIRONNEMENT OPÉRATIONNEL

12. Les OI nous permettent de mener des activités dans des zones d'opération accrues. La zone d'opérations s'étend maintenant au-delà des dimensions physiques tradionnelles que sont le temps, la largeur, la profondeur et la hauteur, et inclue également le spectre électromagnétique (figure 1-2). La zone d'opérations s'étend aussi au-delà des limites physiques des formations déployées tactiquement par le truchement de leurs communications et de leur connectivité avec d'autres éléments des forces terrestres, dans un cadre interarmées et de coalition, comprenant même le Canada à partir du théâtre des opérations. La zone d'opérations est aussi définie par les dimensions humaines, lesquelles incluent non seulement les soldats et les chefs, mais également la population civile du théâtre des opérations, ainsi que les populations canadienne et mondiale. Les zones d'opérations, en particulier celles du niveau opérationnel, seront encadrées non seulement par les éléments traditionnels de la puissance de combat physique, mais aussi par la Déception, les Opérations psychologiques (OPSPSY), la COCIM et les AP.

13. L'influence possible des OI dépend de plus de l'architecture de commandement. Si un adversaire possède une structure de

commandement hiérarchique rigide, la rupture des liens entre la « tête » et le « corps » immobilisera le corps. Dans d'autres situations de conflit, les adversaires peuvent permettre une plus grande autonomie aux commandants d'unité. Dans ce cas, une attaque contre l'autorité centrale pourrait donner aux commandants d'unité l'occasion de faire preuve d'un esprit d'initiative qui pourrait plus que compenser la destruction de l'autorité centrale de coordination. Par exemple, au niveau stratégique, les opérations contre un adversaire suspecté de posséder ou qui possède des armes de destruction de masse pourraient être catastrophiques si elles menaient à la destruction d'un centre de commandement central disposant d'un contrôle intégral sur ces armes de destruction de masse.

14. Les communications mondiales et la technologie de l'information ont accéléré et augmenté la connaissance collective des événements, des problèmes et des préoccupations. Dans le domaine moral, elles allument les passions, créent de nouvelles perspectives, cristallisent des convictions profondes, et amènent les populations, les nations, les organisations et les institutions partout dans le monde à examiner et définir leurs intérêts, et à agir en fonction de ces derniers. Si de nombreux effets de ce phénomène peuvent être bénins et bénéfiques, d'autres créent de l'agitation, de la confusion, du chaos et des conflits. L'univers de l'information illustré dans le présent manuel montre la portée de cet environnement.

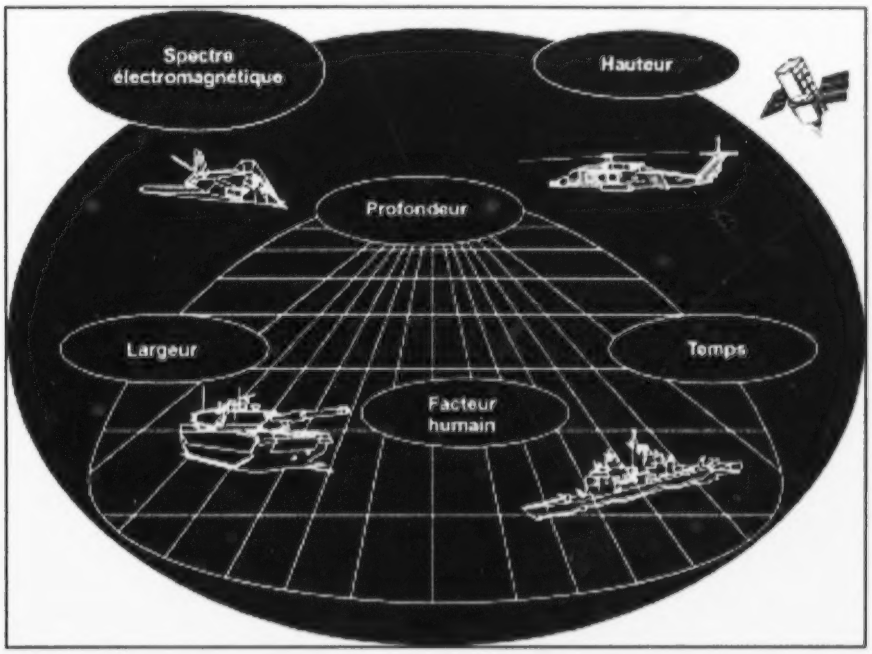

Figure 1-3-2 : La zone d'opérations multidimensionnelle

15. Les OI impliquent donc plus qu'une force qui attaque le flux d'information d'un adversaire tout en protégeant le sien. Elles requièrent une connaissance des sources d'information non militaires et une sensibilité à ces sources. Celles-ci peuvent inclure les organisations gouvernementales et non gouvernementales neutres et amies, y compris les forces paramilitaires, les médias et les organisations politiquement orientées, lesquelles peuvent influer sur les opérations militaires, les perceptions des chefs et le cheminement de l'information au travers des systèmes d'information. Certaines de ces sources d'information peuvent fournir de l'information de niveau tactique presque immédiatement à des auditoires partout dans le monde. De la même manière, des événements lointains peuvent avoir une influence immédiate sur les opérations.

16. L'EGI inclut l'ensemble des individus, systèmes et organisations, la plupart desquels sont situés à l'extérieur des sphères militaire ou gouvernementale. L'EMI est la portion de l'EGI qui est pertinente aux opérations militaires. L'interaction de l'EGI et de l'EMI introduit de nombreux intervenants additionnels dans la zone d'opérations, comprime les niveaux traditionnels de conflit dans le temps, mais les augmente dans l'espace, et donne aux opérations un caractère simultané et continu. Les opérations militaires tactiques sont plus susceptibles d'avoir des

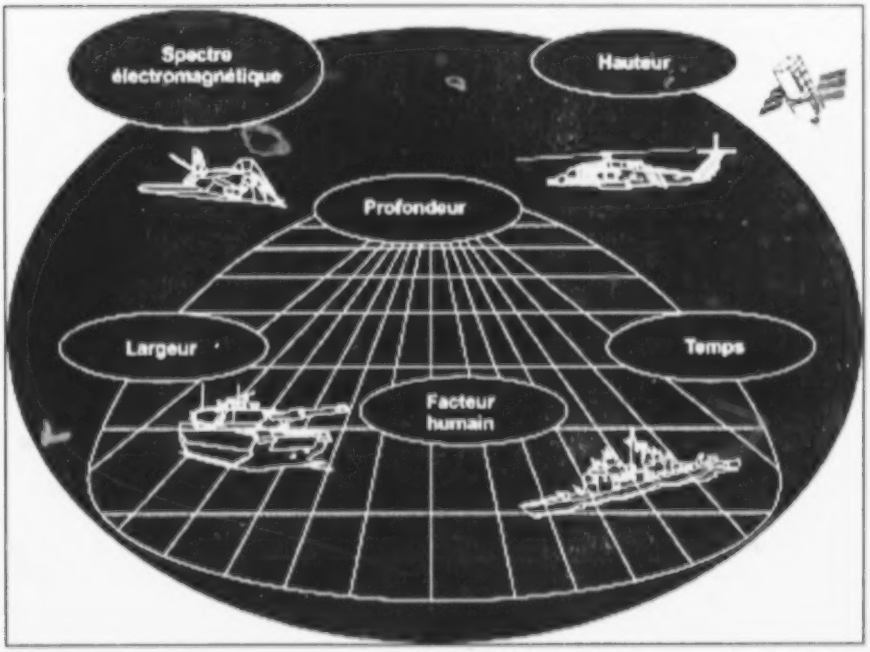

Figure 1-3-2 : La zone d'opérations multidimensionnelle

15. Les OI impliquent donc plus qu'une force qui attaque le flux d'information d'un adversaire tout en protégeant le sien. Elles requièrent une connaissance des sources d'information non militaires et une sensibilité à ces sources. Celles-ci peuvent inclure les organisations gouvernementales et non gouvernementales neutres et amies, y compris les forces paramilitaires, les médias et les organisations politiquement orientées, lesquelles peuvent influer sur les opérations militaires, les perceptions des chefs et le cheminement de l'information au travers des systèmes d'information. Certaines de ces sources d'information peuvent fournir de l'information de niveau tactique presque immédiatement à des auditoires partout dans le monde. De la même manière, des événements lointains peuvent avoir une influence immédiate sur les opérations.

16. L'EGI inclut l'ensemble des individus, systèmes et organisations, la plupart desquels sont situés à l'extérieur des sphères militaire ou gouvernementale. L'EMI est la portion de l'EGI qui est pertinente aux opérations militaires. L'interaction de l'EGI et de l'EMI introduit de nombreux intervenants additionnels dans la zone d'opérations, comprime les niveaux traditionnels de conflit dans le temps, mais les augmente dans l'espace, et donne aux opérations un caractère simultané et continu. Les opérations militaires tactiques sont plus susceptibles d'avoir des

implications politiques et sociales, et exigent ainsi que la planification et l'exécution prennent davantage en compte les facteurs non militaires. Les commandants doivent comprendre l'état final civil et militaire dans son ensemble, et non pas seulement les conditions militaires de cet état final.

SECTION 4
TECHNOLOGIE

17. Comme nous l'avons mentionné précédemment, les nouvelles technologies ont révolutionné l'univers de l'information et l'EMI. Les zones d'opérations et d'intérêt se sont agrandies à tous les niveaux de commandement, principalement en raison des niveaux moindres des forces, de leur plus grande mobilité, des possibilités accrues des systèmes d'armes des forces tant amies qu'ennemies, d'une plus grande capacité de perception de la situation, et des possibilités de réseautage des capteurs et de leurs données. La transmission numérique des données augmente considérablement le volume et la vitesse avec laquelle l'information est transmise d'un point/élément à un autre, sur le champ de bataille. Une forme d'agrégation et de fusionnement des données et de l'information doit être effectuée pour éviter une surabondance d'information nouvelle, récurrente, redondante et non pertinente.

18. La capacité de perception de la situation sera possible seulement si l'information fournie est cohérente, pertinente et opportune. L'information qui n'influence pas le facteur temps et celle de nature répétitive peut être compilée par sujet, entité ou date, et stockée jusqu'à ce qu'elle soit nécessaire. L'information d'importance tactique doit être transmise par les moyens les plus rapides possibles, et être présentée dans une forme normalisée qui peut être comprise par tous. Initialement, l'information devrait être triée en fonction de son opportunité, de sa forme et de son exactitude, et être stockée dans une base de données. L'information doit être comparée à d'autres éléments d'information similaires et faire l'objet d'une investigation si elle ne concorde pas avec l'information déjà disponible. Cette information supplémentaire augmentera l'équation informationnelle, mais son analyse pourrait exiger des vérifications additionnelles. Les avantages de cette fusion des données et de l'information sont résumés à la figure 1-3-2.

19. La technologie a également une incidence sur un autre aspect du champ de bataille, à savoir, l'habileté à visualiser le champ de bataille. La visualisation du champ de bataille (VCB) se définit comme étant *« le processus au moyen duquel le commandant acquiert une compréhension claire de l'état actuel de l'adversaire et de l'environnement, imagine l'état final souhaitable et visualise ensuite la séquence des activités*

menant à cet état final ». La VCB se compose de deux éléments principaux : l'art de la VCB, qui est un processus humain qui peut être développé à des degrés divers chez chacun, et la science de la VCB, qui a trait à la technologie en mesure d'accroître les capacités personnelles.

20. La VCB est un important élément de l'habileté à acquérir la supériorité de l'information à des moments et en des points critiques, sur le champ de bataille. Cette supériorité permettra à une force plus petite de rapidement vaincre un ennemi plus nombreux, et aux formations tactiques de faire respecter des zones de séparation étendues ou encore de mener des opérations de secours humanitaire réparties sur le champ de bataille. La science de la VCB se compose de trois éléments principaux.

a. La capacité de perception de la situation, laquelle permet de répondre aux questions :

   (1) Où suis-je?

   (2) Où sont mes amis?

   (3) Où est l'ennemi?

b. La visualisation de l'environnement, laquelle fournit de l'information sur les différents aspects de l'environnement de la conduite des opérations dont, par exemple : l'espace, l'information géospatiale, la géographie, la météorologie, le spectre électromagnétique, la sociologie et l'aspect juridique.

c. La visibilité des ressources, laquelle fournit au commandant un état précis des ressources humaines, matérielles et informationnelles.

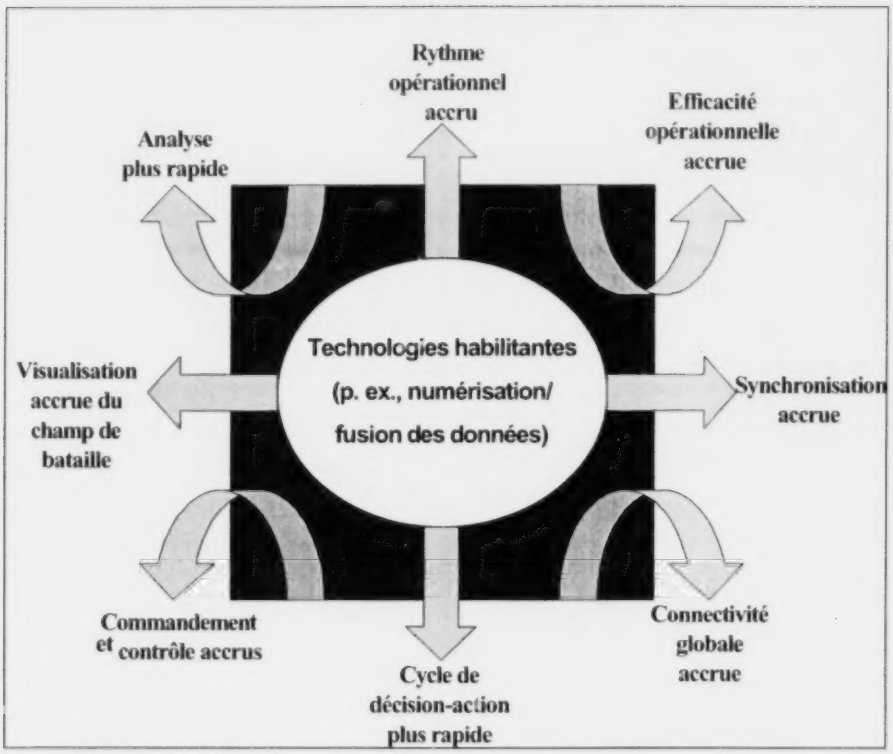

Figure 1-4-3 : Avantages de la fusion des données et de l'information

21. Les progrès réalisés en matière de technologie de l'information ont fourni de nombreux outils, don't les affichages, les capacités de stockage, les bases de données, la recherche et l'extraction de données, la reconnaissance des objectifs, les capteurs et les reseaux (voir la figure 1.4.3). Les compétences nécessaires doivent être acquises rapidement de manière que les progrès technologiques puissant être intégrés au processus des OI. De la même manière, ceux qui ont été choisis pour commander doivent comprendre les processus des OI, et être familiers avec le compétences et technologies sousjacentes, de manière à faire pleinment usage des données pertinentes et à parvenir à une VCB complète.

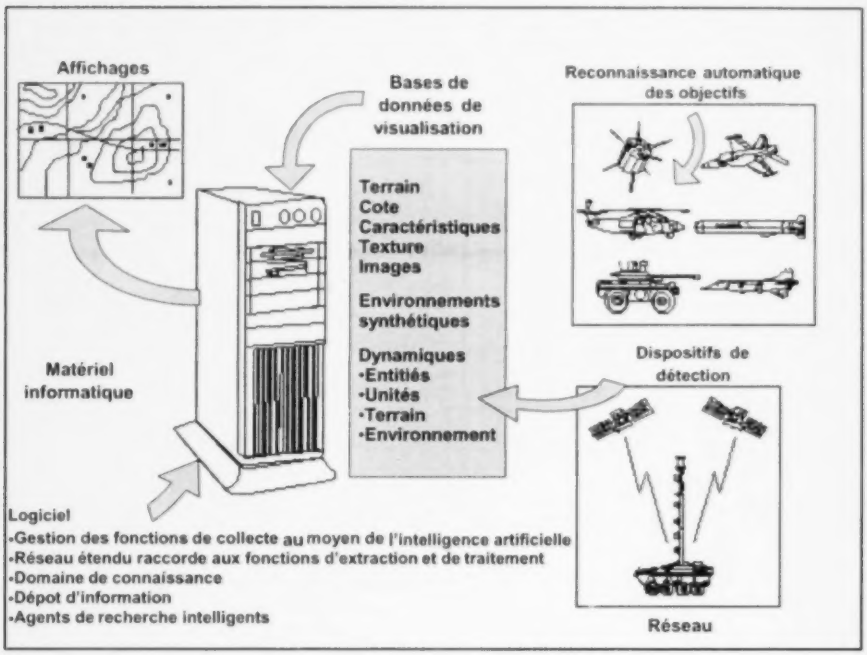

Figure 1-4-4 : Secteurs technologiques clés du point de vue de la visualisation du champ de bataille

22. Un autre secteur clé de croissance, en matière de technologie de l'information, fournit les outils qui aident à passer des données à la compréhension. Les opérations militaires doivent rendre compte d'un environnement fait d'incertitude, de risque et de friction – l'éternel concept clausewitzien du « brouillard de la guerre ». L'information peut être incomplète, non fiable, ambiguë ou même contradictoire. Il existe quatre niveaux d'incertitude :

a. L'incertitude des données relatives à ce qui est observé : ce rapport est-il exact? les forces observent-elles les activités clés?

b. L'incertitude de l'information quant aux faits : où est l'ennemi et en quels nombres?

c. L'incertitude des connaissances quant aux conclusions qu'il convient de tirer des faits connus : quelles sont les intentions de l'ennemi? quel est l'état de son moral?

d. L'incertitude de la compréhension quant à l'issue des actions : les forces peuvent-elles contourner le flanc de

l'ennemi? le succès à ce point-ci entraînera-t-il l'effondrement de l'ennemi?

23. Nombre d'activités militaires sont incertaines parce qu'elles défient toute prévision. De nombreux facteurs ne peuvent pas être prévus ou échappent à la volonté tant des forces amies que de l'adversaire. La technologie de l'information n'éliminera jamais les incidences des incertitudes ni n'éliminera jamais toutes les incertitudes. Elle fournira plutôt aux commandants et à l'état-major des outils leur permettant de « gérer » les incertitudes dans les limites d'un niveau de risque accepté. Lorsque les connaissances et la compréhension font défaut, plus de données peuvent même augmenter l'incertitude.

24. Un des défis importants posés par l'EGI et l'EMI est la sélection et le tri du volume énorme de données auxquelles a accès le commandant. On ne doit pas confondre données et compréhension (voir la figure 1-4-5). Les observations des capteurs qui sont pertinentes pour la zone d'opérations ne sont que des données jusqu'à ce qu'elles soient traitées et prennent une forme organisée et utile. Si la capacité de perception de la situation est essentiellement locale et pertinente pour un échelon donné de la force militaire, la numérisation facilite le partage de la capacité de perception de la situation tant verticalement qu'horizontalement. Le partage de l'information relative à la capacité de perception de la situation renforce la perception globale de la situation et permet une exécution décentralisée dans l'ensemble du commandement.

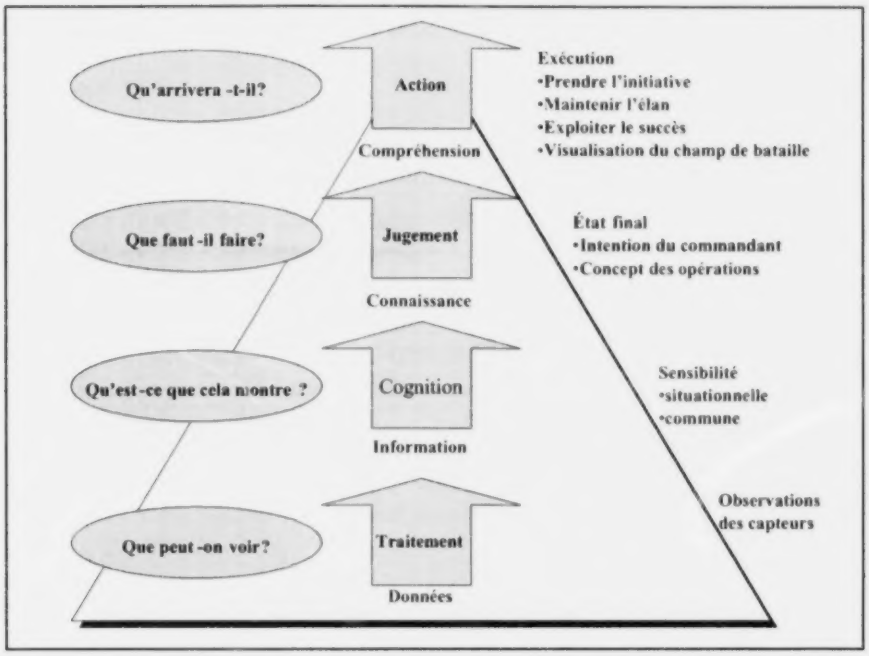

Figure 1-4-5 : La hiérarchie cognitive et l'art des opérations

25. La cognition transforme l'information en connaissance. La connaissance est la base des éléments clés de la conception opérationnelle que sont la mission, l'intention du commandant et le concept des opérations. Parce que la numérisation introduit des liens non hiérarchiques dans une organisation, le commandant se doit encore plus d'exprimer clairement ces éléments du plan. Le jugement informé transforme la connaissance en une compréhension qui permet aux unités de prendre l'initiative, de maintenir leur élan et d'exploiter leurs succès.

26. Le processus de dérivation de la compréhension à partir des données, de l'information et de la connaissance permet au commandant d'instaurer une image commune pertinente dans l'ensemble de la force. Pour aider au processus, le commandant définit les besoins essentiels du commandant en information (BECI).

27. Les BECI sont un outil d'organisation qui visent à assurer la collecte, la production et le suivi de l'information essentielle à l'accomplissement de la mission. Le processus est décrit en détail au chapitre 3. L'information critique peut venir d'organisations gouvernementales ou non gouvernementales amies ou neutres, des médias, et d'organisations orientées politiquement. Toutes ces sources

peuvent avoir une influence sur les opérations militaires, les perceptions des chefs et le flux de l'information dans les systèmes d'information.

28. En concentrant les technologies de l'information aux niveaux appropriées de la hiérarchie cognitive, nous pouvons améliorer la supériorité de l'information, aider à la planification et permettre une exécution rapide. Les secteurs d'amélioration incluent la capacité de :

a. partager verticalement et horizontalement une image commune pertinente qui soit globale et précise;

b. diffuser rapidement les lignes directrices en matière de planification et les options nouvellement générées;

c. évaluer la viabilité des options;

d. calculer les besoins en soutien et en ressources, ainsi que les facteurs temps-distance;

e. aider à visualiser, illustrer, résumer et étudier les options;

f. augmenter la vitesse d'analyse, de compilation et de communication de manière à laisser plus de temps pour la synthèse, laquelle est le processus créatif qui consiste à donner un sens à l'information et à générer les options possibles.

SECTION 5
GESTION DE L'INFORMATION

29. La diffusion et la gestion de l'information sont une responsabilité du commandement. Le succès ou l'échec de la gestion de l'information dépend de la structure de commandement. Si les communications et les systèmes d'information basés sur les technologies de l'information fournissent les moyens qui permettent de traiter, stocker et diffuser l'information, la responsabilité finale de la gestion de l'information repose sur l'utilisateur. Chaque participant à une opération intervient dans le processus de gestion de l'information et est responsable du traitement approprié de la partie de l'information qui relève de l'organisation

30. Si le commandant devait autrefois se battre pour obtenir l'information nécessaire, il est maintenant inondé de données avant même que le combat pour obtenir l'information nécessaire commence. Le flux de l'information au sein de l'organisation est complexe, mais vital du point de vue de l'élaboration d'une image claire de la situation à l'intention du commandant. Un flux optimal de l'information au sein de

l'organisation exige que le transfert s'effectue tant avec rapidité qu'avec clarté tout en évitant une surabondance de données fragmentées ou inutiles. L'organisation élabore un plan de gestion de l'information qui établit les responsabilités et fournit des instructions sur la gestion de l'information. Ce plan est le *« schéma de manœuvre »* applicable au traitement de l'information au sein de l'organisation. Le plan de gestion de l'information doit être intégré aux autres éléments du plan du commandant. Étant donné le volume et le flux accrus d'information auxquels font face les commandants et les officiers d'état-major, le plan de gestion de l'information ne doit pas être traité comme un plan secondaire nécessitant une attention limitée, mais comme un élément primordial du plan du commandant exigeant l'attention spécifique de l'état-major.

CHAPITRE 2
PRINCIPES DE BASE, ÉLÉMENTS ET ACTIVITÉS

SECTION 1
INTRODUCTION

1. Le présent chapitre vise à définir la nature de l'information et à décrire les principes de base des Opérations d'information (OI). On y examine les différents éléments de la fonction de combat des OI, ainsi que les quatre activités critiques essentielles à la conduite des OI. L'intégration des OI aux cinq autres fonctions de combat est essentielle à la production de la puissance de combat.

SECTION 2
PRINCIPES DE BASE

2. L'information est « l'ensemble des données traitées et structurées de toute nature qui peuvent être utilisées dans le cadre des opérations ». Une donnée peut être utilisable en elle-même, mais les données doivent généralement être traitées (placées en contexte) et présentées sous une forme utilisable pour devenir de l'information.

3. Pour que l'information devienne utile, elle doit être évaluée. L'information peut être vraie ou fausse, exacte ou inexacte, confirmée ou non confirmée, pertinente ou non pertinente, et positive ou négative. L'information qui a été évaluée devient de la connaissance. Lorsque nous appliquons le jugement à la connaissance, nous obtenons la compréhension. Et la compréhension est la base des plans militaires.

4. Les OI « *sont des opérations militaires permanentes, à l'intérieur de l'environnement militaire de l'information; elles permettent, améliorent et protègent la tenue du cycle de décision-action du commandant et l'exécution de l'opération, et procurent dans toute la gamme des opérations militaires un avantage pour ce qui est de l'information. Elles comportent des interactions avec l'environnement global de l'information et l'exploitation et l'attaque des systèmes d'information et de prise de décisions de l'adversaire.* »[3]

---

[3] B-GL-300-001/FP-000, *Conduite des opérations terrestres – Doctrine opérationnelle de l'Armée de terre canadienne.*

SECTION 3
ÉLÉMENTS

5. La fonction de combat des OI se compose de six éléments regroupés comme suit :

a. Quatre éléments de soutien :

(1) les systèmes d'information et de communication (SIC);

(2) l'information pertinente, y compris le renseignement, la surveillance, l'acquisition des objectifs et la reconnaissance (système ISTAR);

(3) la coopération civile-militaire (COCIM);

(4) les affaires publiques (AP).

b. Deux éléments d'action :

(1) les Opérations d'information offensives (OI off);

(2) les Opérations d'information défensives (OI déf) (voir la figure 2-3-1).

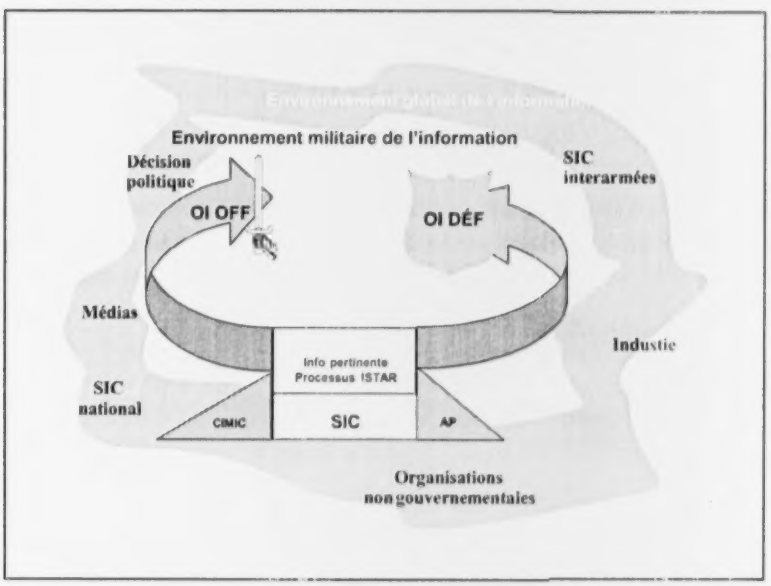

Figure 2-3-1 : Environnement global de l'information

SECTION 3
ÉLÉMENTS

5. La fonction de combat des OI se compose de six éléments regroupés comme suit :

a. Quatre éléments de soutien :

(1) les systèmes d'information et de communication (SIC);

(2) l'information pertinente, y compris le renseignement, la surveillance, l'acquisition des objectifs et la reconnaissance (système ISTAR);

(3) la coopération civile-militaire (COCIM);

(4) les affaires publiques (AP).

b. Deux éléments d'action :

(1) les Opérations d'information offensives (OI off);

(2) les Opérations d'information défensives (OI déf) (voir la figure 2-3-1).

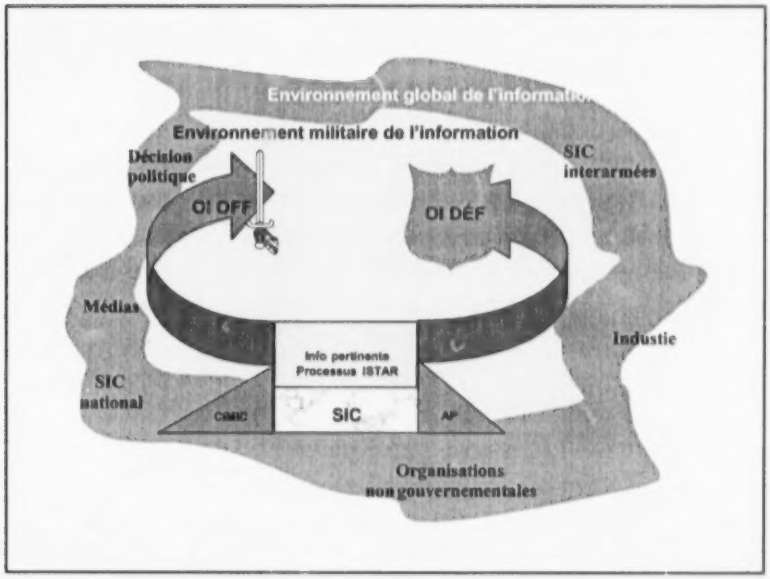

Figure 2-3-1 : Environnement global de l'information

SYSTÈMES D'INFORMATION ET DE COMMUNICATION

6. Les SIC colligent, traitent, stockent et diffusent l'information relative aux opérations courantes et futures. L'automatisation a fait de grands progrès en matière de traitement de l'information, mais les humains demeurent les plus efficaces lorsqu'il s'agit de déterminer la pertinence de l'information et d'en faire la synthèse. Les SIC sont les moyens qui permettent aux commandants et à leurs officiers d'état-major de :

a. gérer l'information;

b. suivre la situation actuelle;

c. intégrer et coordonner les opérations de l'ensemble des fonctions de combat;

d. coordonner le soutien interarmées;

e. mettre à jour les paramètres de visée des systèmes d'armes;

f. contrôler les opérations proches, en profondeur et arrière comme s'il s'agissait d'un cadre opérationnel unique.

ARCHITECTURE

7. Les SIC sont essentiels à l'application efficace de la puissance militaire. L'évolution de l'architecture globale de commandement et d'information de l'Armée de terre, avec ses trois aspects complémentaires axés sur les questions opérationnelles, systémiques et techniques, est d'une importance particulière pour les SIC. L'objectif de cette initiative est de créer un environnement opérationnel commun de systèmes normalisés interactifs et de modèles en vue de la collecte, du stockage et de la manipulation de la totalité de l'information de l'Armée de terre.

8. **Architecture opérationnelle**. L'aspect opérationnel de l'architecture globale de commandement et d'information établit la connectivité requise entre les processus, fonctions, données et organisations de notre système d'information de commandement et de contrôle (SICC). Il montre ce que nous faisons, de quelle l'information nous avons besoin pour le faire, à quelle fréquence et avec qui nous devons échanger de l'information, et comment nous avons l'intention de gérer notre fonds d'information.

9. **Architecture de système**. L'aspect architecture de système de l'architecture globale de commandement et d'information détermine les liens entre les composantes du système d'information de commandement et de contrôle (SICC), et les connexions requises. Il utilise un contexte organisationnel pour montrer les structures d'affectation et de réseau, et appuie les décisions techniques en matière de protocoles d'information et de largeur de bande, par exemple.

10. **Architecture technique**. L'aspect architecture technique de l'architecture globale de commandement et d'information établit les règles gouvernant l'agencement, l'interaction et l'interdépendance de l'ensemble des parties et éléments de notre SIC. Il spécifie les normes admissibles de conception des composantes du SIC et est d'une importance critique pour la création et le maintien des systèmes interactifs.

INTÉGRATION

11. L'intégration verticale la et horizontale du SIC facilite l'agilité, l'initiative, la profondeur, la synchronisation et la versatilité tactiques et opérationnelles. Cette intégration est essentielle au succès de l'Armée de terre dans les opérations interarmées et interarmes.

CONNECTIVITÉ GLOBALE

12. La connectivité globale est essentielle à l'établissement des liens entre les aspects stratégiques, opérationnels et tactiques des OI, ainsi qu'à la capacité de déploiement des forces à l'échelle mondiale. Le SIC soutient les opérations au niveau mondial au moyen de systèmes basés tant dans l'espace que sur le terrain. Le SIC doit être configuré de manière à fournir le soutien requis en information avec un minimum de repositionnement, que ce soit au cours d'une phase de déploiement stratégique ou en cas de préparation à une attaque tactique. Les SIC tant militaires que commerciaux jouent un rôle important dans cette architecture.

13. L'Armée de terre utilise les technologies de l'information sur le champ de bataille pour fournir une structure intégrée de commandement et de contrôle. L'Armée de terre effectue actuellement la transition de son système manuel de commandement et de contrôle à un système commun à trois niveaux avec applications spécialisées connexes qui fonctionnera de façon décloisonnée dans les bases et sur le terrain. Ce système commun utilise des services de communication commerciaux et des communications militaires multinationales par satellite, et se sert du

Système tactique de commandement, de contrôle et de communication (STCCC) comme porteur d'information. Ce système commun est complété lorsqu'il y a lieu par des applications spécialisées visant à répondre à des besoins d'information ou de traitement spécifiques. L'intégration d'un SIC moderne à nos unités tactiques continuera d'améliorer la connectivité de ces dernières, le processus de prise de décisions et, en fin de compte, la létalité, la surviabilité et la capacité de diriger le rythme des opérations. Le SIC de l'Armée de terre est étudié au chapitre 3.

14. Les communications doivent permettre la diffusion à haute vitesse de l'information. Celle-ci est réalisée par l'utilisation combinée de la communication hiérarchique et de la communication à multidiffusion. La communication hiérarchique est bien comprise, puisqu'il s'agit de l'approche classique en matière de communications militaires, et est essentielle à la diffusion de l'information, laquelle doit être effectuée par les voies connues. La communication à multidiffusion, qui permet d'éliminer les obstacles organisationnels et, ainsi, les délais dans la diffusion de l'information commune et non hiérarchique, est actuellement intégrée à un degré moindre. La communication à multidiffusion permet la transmission descendante directe simultanée de données ou d'information à des échelons multiples à partir de divers capteurs ou bases de données, de même que la diffusion de produits d'information finis aux forces déployées à partir d'organisations du théâtre des opérations, ministérielles ou nationales. L'information peut être fournie aux forces déployées par des moyens électroniques.

GESTION DE L'INFORMATION

15. La nécessité de gérer l'information n'est pas nouvelle; le volume et les divers types d'information à gérer pour assurer le succès des opérations augmentent toutefois de façon exponentielle. Pour gérer l'information avec succès, nous devons adopter une approche holistique en ce qui touche la gestion de l'information de tous les types, formes et utilités. Notre but doit être de minimiser la duplication de l'information et des efforts, ainsi que la perte d'information, tout en maximisant la qualité, l'opportunité et l'intégrité de l'information, de même que la vitesse d'accès à cette dernière. La gestion de l'information est étudiée plus en détail dans la B-GL-331-001/FP-001, *Doctrine de soutien du commandement*.

INFORMATION PERTINENTE

16. Tout au long de l'histoire de la guerre, les commandants se sont efforcés de déterminer comment utiliser au mieux l'information disponible. La volonté de recueillir le plus d'information possible sur l'emplacement, l'efficacité au combat et l'activité de leurs propres forces, ainsi que sur l'emplacement, la disposition, l'efficacité et les intentions de l'ennemi, est une caractéristique constante des commandants victorieux, quelle que soit l'époque ou le pays. Aujourd'hui, les commandants agissent dans un environnement marqué par une augmentation massive de la quantité d'information, ainsi que par la rapidité avec laquelle l'information est recueillie et les décisions sont diffusées. Ces décisions et cette information peuvent avoir des répercussions immédiates sur les niveaux stratégique, opérationnel ou tactique quels qu'en soient le point ou niveau d'origine. L'expansion exponentielle de l'EMI a rendu les opérations militaires plus dépendantes que jamais d'organisations, de systèmes et d'individus qui n'appartiennent pas au militaire. Ces dépendances ont rendu l'EMI d'un commandant plus vulnérable que jamais à un adversaire.

17. La collecte, l'utilisation et la diffusion d'information pertinente sont basées sur l'intégration systématique et la coordination de l'information sans égard à la source ou au moyen de collecte. L'information pertinente est fusionnée de manière que le commandant puisse avoir une compréhension approfondie de la situation présente et déterminer l'aspect futur de sa zone d'opérations. Lorsqu'elle est diffusée dans l'ensemble de la force, cette compréhension commune de la situation contribue à la cohésion et permet aux subordonnés de bien comprendre l'intention du commandant et, de ce fait, l'effort principal. Ce point est critique à la philosophie de commandement de l'Armée de terre canadienne.

18. L'information pertinente inclut la totalité de l'information dans l'EMI d'un commandant. Elle inclut l'information fournie par la force amie en réponse aux demandes du commandant, l'intention et le concept des opérations du commandant supérieur, ainsi que l'information relative à divers autres groupes dans le conflit (leurs chefs militaires et politiques, leurs motifs, leurs traditions, leurs institutions, leur culture, leur langue et leur histoire). Le renseignement est la partie de l'information pertinente qui a trait à l'adversaire (ou à l'adversaire possible), aux conditions climatiques et au terrain. Le renseignement prend une importance accrue, et même cruciale, à l'âge de l'information. Parce que la zone d'opérations bénéficie grâce aux OI d'une connectivité mondiale, l'information sur les adversaires actuels ou possibles doit être élaborée à l'échelle mondiale.

L'interaction avec l'EMI requiert de l'information opportune sur de nombreux aspects des adversaires actuels ou possibles, notamment les aspects culturels, politiques et commerciaux.

19. Les commandants doivent disposer d'information pour commander. L'information permet la mise en œuvre du cycle de décision-action du commandant et procure une orientation aux forces dans l'exécution de leur mission opérationnelle. La collecte, le traitement et la diffusion de l'information sont critiques à l'atteinte d'une capacité de perception de la situation dans l'ensemble de la force, laquelle sensibilité favorise une unité de l'effort dans l'exécution de la mission. Le commandant fonctionne dans le contexte de l'EGI, et ajuste son EMI de manière à améliorer sa capacité de perception de la situation comme il convient pour l'opération en cours.

20. On trouvera dans la B-GL-300-003/FP-000, *Commandement*, chapitre 3, annexe A, un inventaire des besoins d'information des commandants. Les commandants déterminent l'information critique pour chaque opération et publient ces exigences sous la forme de besoins essentiels du commandant en information (BECI). Seul le commandant peut décider de l'information essentielle sur la base de la mission, de l'expérience et des intentions du commandant supérieur. Le personnel peut seulement recommander des BECI au commandant sous la forme de :

a. Besoins prioritaires en renseignement (BPR) visant à déterminer ce que le commandant veut ou doit savoir sur l'ennemi, ses intentions et/ou le terrain (comment je vois l'ennemi).

b. Besoins en information sur les forces amies (BIFA) visant à permettre au commandant de déterminer le potentiel de combat de la ou des unités amies adjacentes (comment je me vois).

c. Éléments essentiels d'information sur les forces amies (EEIFA) visant à permettre au commandant de déterminer comment il doit protéger la force des systèmes de collecte d'information de l'action de l'ennemi (comment je peux empêcher l'ennemi de me voir).

21. Une analyse tactique graphique (ATG) exacte de l'EMI est une des clés du succès des opérations. L'information pertinente, incluant la collecte de données de renseignement et le soutien des opérations, commence en temps de paix et doit être continue tout au long des différentes phases d'une opération ou d'une campagne. Les progrès en

matière de technologie de l'information permettent de changer la façon dont l'information est fournie au soutien des opérations.

22. Des OI fructueuses requièrent la fusion de l'information en provenance d'une variété de sources. Les progrès dans le domaine de la détection, des processeurs et des communications sont combinés de manière à assurer une reconnaissance et une surveillance détaillées et rapides de presque tout endroit du globe. Tant les sources militaires que non militaires fournissent des données qui peuvent servir à produire de l'information et du renseignement. Les sources non secrètes d'information et de renseignement fourniront une bonne partie de l'attirail de guerre et des données techniques. Une bonne intégration des OI requiert également que l'ATG soit basée sur la compréhension approfondie du potentiel et du style de processus décisionnel de l'adversaire. L'information pertinente en tant que composant des OI est étudiée en détail au chapitre 4.

23. Le processus ISTAR est le système au moyen duquel le commandant effectue sa propre collecte d'information dans le cadre du processus de collecte de l'information pertinente. Dans l'environnement moderne, la différence entre les types de capteur et la connaissance de qui les commande deviennent moins importantes. C'est l'information qui importe. Un seul capteur peut recueillir simultanément une gamme étendue d'information pour de nombreux utilisateurs sans que les besoins de l'utilisateur principal en souffrent aucunement. Le système ISTAR est décrit en détail au chapitre 5.

AFFAIRES PUBLIQUES

24. Dans l'histoire récente, le succès ou l'échec des opérations militaires ont été grandement influencés par le fait que la population croyait ou non que la mission était une réussite. L'Armée de terre a connu un succès plus que mitigé dans le domaine des affaires publiques, ce qui a nui à la réputation et à l'efficacité opérationnelle des Forces canadiennes. La plupart des opérations militaires sont conduites sous le regard attentif de la population. La couverture médiatique nationale et internationale joue un rôle majeur dans la naissance rapide d'un débat public et la formation de l'opinion publique. Les médias d'information servent de tribune publique pour l'analyse et la critique des buts, objectifs et actions. Ils peuvent avoir un effet sur la planification et les décisions politiques, stratégiques et opérationnelles, ainsi que sur la réussite ou l'échec de la mission.

25. La réalité de l'information, qui est transmise en temps presque réel à des vitesses plus grandes et à des auditoires plus larges que par le passé, a comblé l'écart entre ce qui se produit sur le terrain, et les buts et objectifs d'un point de vue national. Les affaires publiques sont une responsabilité du commandant. L'officier d'affaires publiques (OAP) aide le commandant à suivre les perceptions du public, et à élaborer et diffuser des messages clairs et objectifs en accord avec ses intentions, relativement aux opérations militaires. L'objectif des affaires publiques est d'aider à assurer la supériorité de l'information en prenant l'initiative du point de vue des activités médiatiques et en mettant en place des programmes qui :

a. Protègent les soldats des effets de la propagande, de la désinformation et des rumeurs ennemies, car des soldats bien informés sont des soldats efficaces.

b. Favorisent la production de comptes rendus, ainsi qu'un accès aux unités et aux soldats, ouverts et indépendants.

c. Établissent les conditions menant à un climat de confiance dans l'Armée de terre.

d. Fournissent une information équilibrée, juste et crédible sur les opérations de l'Armée de terre grâce à la diffusion rapide d'une information complète, précise et opportune à la population dans la zone d'opérations, au Canada et dans le monde.

26. Les commandants se servent de leurs programmes d'information interne pour informer les soldats de leur rôle, de ce qui est attendu d'eux et de la façon dont ils aident à l'exécution de la mission. Cette information aide également les soldats à combattre les effets de la propagande ou de la désinformation ennemies. Les commandants, par l'entremise de leur OAP, lancent et dirigent des programmes d'information interne. Chaque soldat doit recevoir l'information spécifique à l'opération par les voies hiérarchiques, de même que par le truchement des nouvelles internationales, nationales et locales. Les médias sont une importante voie d'information de la population. Les commandants, officiers d'état-major et soldats doivent toutefois tenir compte de la sécurité opérationnelle et des autres exigences opérationnelles lorsqu'ils travaillent avec les médias.

27. Le personnel d'AP soutient les commandants en évaluant l'environnement informationnel, en les avisant des implications des opérations courantes et futures du point de vue des affaires publiques, et en diffusant le plan d'affaires publiques au soutien de ces opérations. Les

commandants comprennent l'importance d'une présentation équilibrée, juste et crédible de l'information tant aux auditoires internes qu'externes. Les commandants intègrent les affaires publiques à leur processus de prise de décisions en tenant compte de cette dimension dans leur évaluation de la situation de même que dans l'élaboration de leurs plans d'action et de leurs ordres. Pour une étude plus détaillée de la question, voir le chapitre 7.

COOPÉRATION CIVILO-MILITAIRE

28. La COCIM fournit l'interface entre les acteurs et influences critiques dans l'EGI. Que ce soit en temps de paix, de conflit ou de guerre, la conduite fructueuse d'une opération dépend souvent du soutien de la COCIM. Dans certains cas, la COCIM peut même être l'effort principal. Quoique les conditions diffèrent selon le type de conflit, les activités de COCIM établissent, maintiennent, influencent ou exploitent les relations entre les forces militaires, les autorités civiles et la population dans une zone d'opérations, facilitant ainsi ces dernières.

29. Le personnel de COCIM doit dialoguer avec les acteurs et éléments d'influence clés au sein de l'EGI, comme les ONG et les autorités locales. Les éléments de COCIM soutiennent les opérations militaires en appliquant leurs compétences et expérience de l'administration publique, de l'économie, des installations publiques, de la linguistique, des affaires culturelles et de l'information civile du pays hôte, et en recueillant de l'information pertinente du point de vue des BECI. Le personnel de COCIM joue un rôle complexe et important en fournissant de l'information tant pour le cycle de renseignement que le cycle de planification des opérations. Pour une étude plus détaillée de la COCIM, se reporter au chapitre 8.

OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES

30. Aujourd'hui, la complexité et l'étendue de l'EMI font en sorte qu'il est plus difficile de briser le potentiel d'un adversaire au moyen d'une seule attaque ou application de la puissance de combat. L'intégration et la coordination efficaces des OI contribuent en conséquence de manière importante à maximiser les résultats des attaques. De la même manière, une intégration soignée est également nécessaire à la protection de nos systèmes et processus critiques contre les attaques ennemies. Sans une intégration et une coordination complètes des OI

offensives et défensives, l'efficacité opérationnelle sera réduite et nos points vulnérables seront exposés.

OPÉRATIONS D'INFORMATION OFFENSIVES

31. Le but des OI offensives est de parvenir à contrôler la fonction de commandement de notre adversaire, et d'influencer l'ennemi et les personnes neutres sur les plans tant du flux d'information que du niveau de capacité de perception de la situation. Des OI offensives efficaces empêchent l'ennemi d'exercer un commandement et un contrôle efficaces, ou nous permettent d'avoir prise sur son évaluation de la réalité.

32. Les OI offensives peuvent frapper le potentiel d'un adversaire à tous les échelons, ciblant le personnel, le matériel, les communications et les installations dans un effort de perturbation ou d'influence des opérations. L'information pertinente, y compris l'ISTAR, joue un rôle clé dans la planification des OI offensives et les opérations, avec la création et la mise à jour de bases de données régionales sur les influences personnelles, historiques et culturelles, les ATG, et les évaluations des dommages au combat (EDC) tant de types neutralisation par déroutement que destruction matérielle. La principale approche, en matière d'influence de l'adversaire, est l'application coordonnée des quatre activités d'information décrites à la section 4 du présent chapitre.

OPÉRATIONS D'INFORMATION DÉFENSIVES

33. Les OI défensives visent à maintenir un commandement et un contrôle efficaces des forces amies en niant ou tournant à l'avantage de ces dernières les efforts de l'adversaire pour influencer, détériorer ou détruire les systèmes de commandement et de contrôle amis, et ce, tout en protégeant nos soldats, la population neutre et notre propre population contre les effets des OI offensives de l'ennemi. Les OI défensives se subdivisent en mesures actives et passives, et visent à limiter la vulnérabilité des forces (personnel, matériel et information) aux actions hostiles, même lorsque les forces déployées font face à des menaces et à un potentiel croissants de l'ennemi. Les OI défensives incluent la lutte contre la propagande et les opérations psychologiques (OPSPSY) de l'adversaire de manière à éviter qu'elles aient une incidence sur les opérations, options et opinion publique amies, de même que sur le moral des troupes amies.

SECTION 4
ACTIVITÉS

34. Les OI incluent l'acquisition, l'utilisation, la protection et le refus de l'information. Lorsqu'elles sont exécutées efficacement, ces activités critiques constituent un complément aux habiletés en matière de commandement, accélèrent la prise de décision, minimisent l'incertitude, concentrent la puissance de combat, protègent les forces, exploitent le potentiel organisationnel, font le lien entre l'EMI et l'EGI, et améliorent la capacité de perception de la situation. Ces activités s'appliquent tant à l'information qu'aux systèmes de communication et d'information (matériel, personnel, organisations et procédés). Même si elles sont énumérées de façon séquentielle, ces activités sont concomitantes et décloisonnées dans leur application (voir la figure 2-4-2).

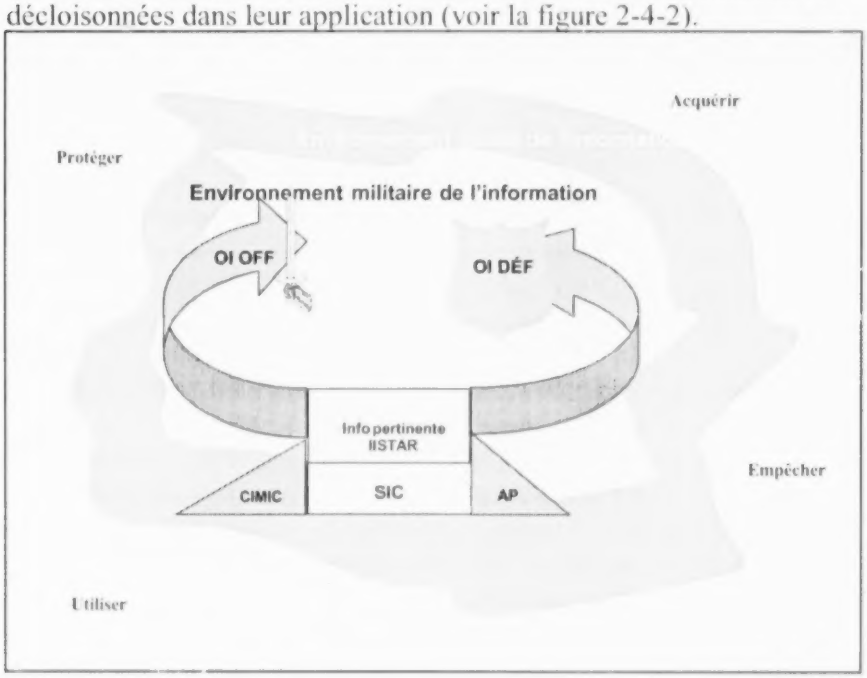

Figure 2-4-2 : Activités d'opérations d'information

ACQUÉRIR

35. Les commandants doivent prendre en compte la nature de l'information requise avant d'affecter les ressources en vue de son acquisition. Les questions initiales incluent :

SECTION 4
ACTIVITÉS

34. Les OI incluent l'acquisition, l'utilisation, la protection et le refus de l'information. Lorsqu'elles sont exécutées efficacement, ces activités critiques constituent un complément aux habiletés en matière de commandement, accélèrent la prise de décision, minimisent l'incertitude, concentrent la puissance de combat, protègent les forces, exploitent le potentiel organisationnel, font le lien entre l'EMI et l'EGI, et améliorent la capacité de perception de la situation. Ces activités s'appliquent tant à l'information qu'aux systèmes de communication et d'information (matériel, personnel, organisations et procédés). Même si elles sont énumérées de façon séquentielle, ces activités sont concomitantes et décloisonnées dans leur application (voir la figure 2-4-2).

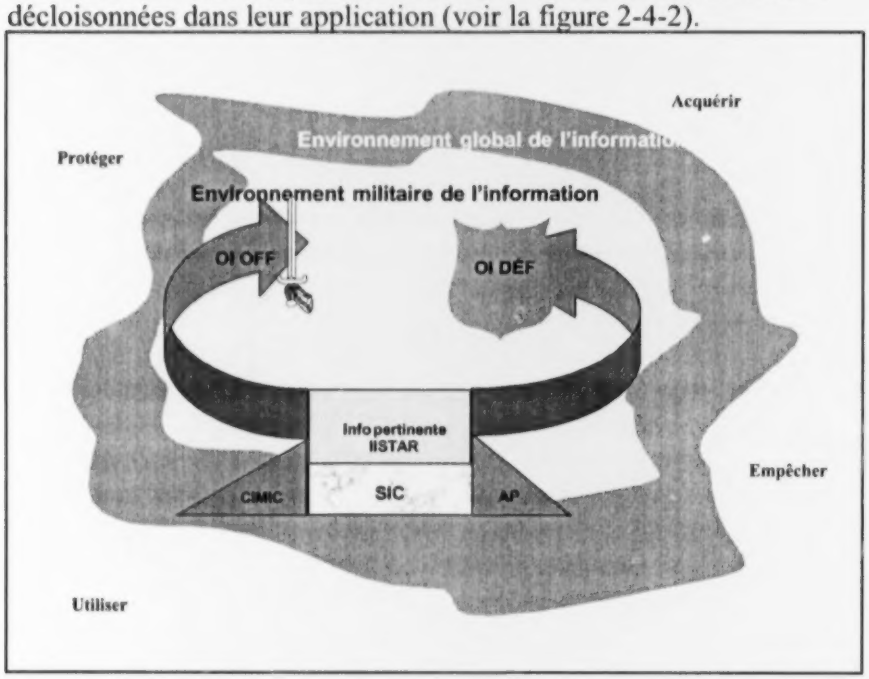

Figure 2-4-2 : Activités d'opérations d'information

ACQUÉRIR

35. Les commandants doivent prendre en compte la nature de l'information requise avant d'affecter les ressources en vue de son acquisition. Les questions initiales incluent :

a. Qu'est-ce que je sais déjà?

b. De quelle information ai-je besoin?

c. Quelle est la nature de cette information?

d. Comment cette information peut-elle être acquise?

36. Les BECI seront normalement formulés dans le cadre de l'estimation du commandant et articulés par le truchement d'ordres. L'information est également acquise au moyen d'un cycle de collecte d'information plus générale axé sur la compilation d'information pertinente en provenance d'autres sources et influences dans l'EMI. Les besoins d'information du commandant ne sont pas satisfaits par une source unique, mais par :

a. une combinaison de ses propres systèmes d'ISTAR;

b. des mises à jour de la situation tactique de l'unité;

c. des activités humaines de renseignement (HUMINT);

d. des agences stratégiques ou nationales (renseignement, affaires extérieures et autres);

e. une interface avec les populations, forces de police et médias d'information locaux;

f. l'EGI.

UTILISER

37. Les commandants disposeront dans le futur d'une quantité sans précédent d'information. Autrefois, le problème des commandants était de faire l'acquisition d'une information opportune et exacte. Le problème du commandant d'aujourd'hui est la surabondance de l'information. Utiliser l'information signifie exploiter, analyser, vérifier, mettre à jour et gérer (déplacer, stocker et présenter) l'information. Le résultat est une capacité de perception de la situation commune et la possession des connaissances nécessaires à la planification des opérations futures. Le commandant peut voir sa zone d'opérations grâce à l'utilisation de systèmes spatiaux, aériens et terrestres qui font l'acquisition de l'information pertinente et fournissent un tableau de la situation courante. Le commandant étend sa réflexion à tous les SIC et organisations accessibles de l'EGI. Une fois les données acquises, analysées et colligées, l'information résultante est utilisée pour la mise à jour et la validation d'une capacité de perception de la situation commune. Cette

sensibilité commune sert de fondement au perfectionnement, à la poursuite ou au rajustement des décisions, plans et opérations :

a. L'information est ciblée et utilisée en vue de l'émission de lignes directrices, de l'établissement des priorités relatives aux ressources et de la définition des exigences.

b. Les officiers d'état-major transforment ensuite les lignes directrices en plans opérationnels ou en ordres d'opération. Ils s'efforcent d'intégrer l'information à tous les échelons et de planifier l'utilisation de toute l'information disponible sans égard à la source.

38. L'information la plus opportune, exacte ou pertinente, en particulier dans le cas des opérations autres que le guerre, peut provenir de sources à l'extérieur de l'unité ou du militaire. Une unité doit tirer parti des SIC tant organiques que non organiques. Les systèmes non organiques peuvent être gouvernementaux ou non gouvernementaux (EGI). L'utilisation de systèmes gouvernementaux autres (MDN et autres ministères) est coordonnée par le QGDN. L'utilisation de systèmes non gouvernementaux est plus complexe. Les unités peuvent utiliser certains services ouvertement et passivement, comme l'écoute ou l'abonnement à des médias radiodiffusés. Elles peuvent également faire usage de services comme les relais de communication et les services de prévision météorologique. Les commandants doivent toutefois être conscients des limites légales et politiques applicables à l'utilisation de tout SIC ne relevant pas du MDN.

39. La façon dont les réseaux d'information d'une organisation sont reliés les uns aux autres peut fournir des conduits multiples pour l'information. L'interréseautage horizontal des SIC aux plus bas niveaux possibles fournit un tableau multidimensionnel et plus élaboré de ces systèmes que ne le ferait un rapport cloisonné classique.

EXPLOITER

40. L'exploitation se définit comme l'activité consistant à « *prendre pleinement avantage de toute information venue à notre connaissance aux fins des opérations militaires* ». Tous les environnements et systèmes d'information qui entourent une opération, qu'ils soient amis ou ennemis, militaires ou non militaires, doivent être vus comme sources d'information à exploiter. L'exploitation de l'information doit être envisagée d'une manière générale et non pas seulement du point de vue du

renseignement. Toute l'information acquise doit être exploitée, ce qui implique :

a. une analyse de l'information;

b. l'accès aux bases de données de soutien;

c. l'accès aux SIC tant militaires que mondiaux;

d. la vérification et la mise à jour de l'information;

e. la présentation de l'information sous une forme utilisable.

41. L'information recueillie sur un adversaire devient, une fois traitée, du renseignement. Le renseignement exige une potection spéciale en raison de sa nature et des moyens par lesquels il été acquis. La collecte d'information et le travail de renseignement doivent commencer en temps de paix de manière à établir l'analyse de la zone d'opérations et le mode de fonctionnement des adversaires possibles. La connaissance de l'infrastructure informationnelle de l'adversaire est aussi importante que la connaissance des stratégies, tactiques, techniques et méthodes d'un adversaire possible. La connaissance de l'infrastructure de l'adversaire permettra une estimation du personnel, des installations, des capteurs, des processeurs et du processus décisionnel.

VÉRIFIER

42. L'exactitude de l'information doit être vérifiée. Dans le passé, l'accent était mis davantage sur la vérification du renseignement. Maintenant, il est devenu d'une importance critique de vérifier la totalité de l'information. L'information est périssable et requiert une mise à jour constante pour demeurer pertinente. Les événements peuvent rendre un élément d'information non pertinent ou à ce point non représentatif qu'il dépeint un tableau inexact de la réalité. L'information en main depuis un ceratin temps peut fausser la capacité de perception de la situation du commandant et nuire à sa capacité de ce dernier de visualiser le champ de bataille. Les processus de planification opérationnelle (PPO), les BECI et les plans, tant les plans opérationnels que les plans de collecte d'information, doivent tous tenir compte de la nature périssable de l'information.

GÉRER

43. Pour servir à la conduite des opérations, l'information doit être coordonnée et synchronisée avec soin. À la lumière des lignes directrices émises, les officiers d'état-major coordonnent et intègrent les besoins d'information de façon à coordonner le flux d'information critique en fonction du concept opérationnel. La gestion de l'information doit être axée sur l'exigence opérationnelle qui consiste à extraire l'information du processus de planification opérationnelle, des systèmes ISTAR, de la contre-ingérence (CI), de la sécurité opérationnelle (SECOP), des communications et des opérations de sécurité.

44. Une gestion efficace de l'information et des ressources permet la circulation horizontale et verticale de l'information entre toutes les fonctions de combat, et, ainsi, une planification, une préparation, une prise de décisions et une exécution efficaces. Elle sert à éliminer les dédoublements et les redondances, et permet aux systèmes de traiter l'information pertinente sensible au facteur temps. Les clés à ces flux efficaces de communication et d'information sont la connectivité, la vitesse de traitement et la résilience. Les unités peuvent gérer la connectivité entre leurs ressources organiques. La difficulté consiste à maintenir une connectivité horizontale et verticale à l'extérieur de l'unité, en particulier dans le cas de forces qui utilisent des systèmes plus anciens basés sur les communications phoniques ou un support papier, ou encore des communications et des SIC différents. La connectivité est assurée grâce au maintien de liens électroniques et humains verticalement et latéralement, à l'extérieur de l'unité. Dans le cas de forces ou unités aux possibilités techniques moins avancées, les équipes doivent être prêtes à déployer des spécialistes ou du personnel de liaison équipés du matériel nécessaire.

45. La résilience est la capacité des SIC, d'un point de vue technique et de gestion, à fournir la connectivité et la continuité nécessaires en cas de dégradation. De plus, les chefs et planificateurs militaires doivent comprendre les mécanismes d'interconnexion et d'interaction de l'information et des systèmes militaires avec l'EGI. Une trop grande dépendance par rapport aux systèmes commerciaux, en particulier les satellites et les réseaux de télécommunications du pays hôte, peuvent imposer des restrictions ou des limitations. Une gestion suivie et une coordination cohérente contribueront à assurer la disponibilité, la fiabilité et la rapidité des systèmes d'aide au commandement.

PROTÉGER

46. Si la prolifération de l'information et des technologies de l'information peut être un grand avantage, elle constitue également un risque potentiellement important dont on doit tenir compte dans chaque opération. La protection des soldats et du matériel, si elle n'est pas nouvelle, a pris plus d'importance dans l'environnement riche en information dans lequel nous vivons. L'information et les SIC amis doivent être protégés dans l'ensemble de la zone d'opérations. D'un point de vue opérationnel, la protection de l'information requiert une évaluation des vulnérabilités amies du point de vue des OI offensives de l'ennemi. Les commandants doivent évaluer la vulnérabilité de leurs soldats et systèmes à une exploitation ou une attaque par un ennemi capable d'attaquer les systèmes de commandement et de contrôle et le personnel amis sur un large front au moyen de mesures de guerre électronique, de destruction matérielle, de déception et de désinformation.

47. Pour arrêter ou retarder le fonctionnement d'une arme ou d'un système, un adversaire peut attaquer l'information ou le SIC qui valident ce système. Par exemple, un adversaire peut introduire, par l'entremise d'un réseau de télécommunications, un code logiciel nuisible directement dans le SIC de manière à empêcher le partage de l'information de combat avec les autres systèmes de l'Armée de terre et interarmées. Les mesures visant à protéger un fonctionnement sans contrainte dans le cadre de l'EMI sont considérées comme faisant partie des OI défensives.

48. L'information pertinente et les SIC de soutien doivent être protégés aux niveaux électronique, matériel et humain, par rapport à la menace possible sans que cette protection nuise à l'ensemble de l'opération. Les programmes de sécurité qui déterminent les menaces aux systèmes de commandement et d'aide au commandement prennent également une importance accrue dans les bases parce que la nature poreuse et ouverte de l'EGI rend l'infrastructure informationnelle d'aide au commandement vulnérable en tout temps aux attaques ou à son exploitation. Dans le cadre des activités de planification des opérations tant en campagne que dans les bases, les commandants à tous les niveaux doivent analyser la structure d'information de l'unité afin de trouver les points faibles critiques et de fournir la protection nécessaire. Il n'est pas possible de tout protéger. Les commandants doivent en conséquence effectuer une analyse de gestion des risques dans le but de déterminer l'information et les SIC essentiels qu'il importe de protéger de toute perturbation ou corruption. Cette analyse mènera également à l'établissement des priorités relatives aux opérations de sécurité.

49. Les données, les ordinateurs, les systèmes de communication et les installations de soutien sont les éléments d'infrastructure dont la protection est nécessaire. Les planificateurs doivent intégrer les divers éléments de l'EGI aux plans pour assurer que les commandants prennent en considération les incidences de fait ou possibles de ces éléments sur toute opération. Il convient en outre d'effectuer une évaluation et une analyse des points faibles de manière à disposer des données opportunes et exactes nécessaires à la détermination des menaces de fait ou possibles à l'endroit des SIC amis.

50. La protection des ordinateurs et des systèmes de communication contre une intrusion, une perturbation et une destruction par l'ennemi est une étape de base initiale de toute approche de protection d'ensemble. Les commandants doivent toutefois réagir aux tentatives de déception et de propagande de l'ennemi. Un ennemi futé peut se servir de propagande pour prédisposer un commandant et son état-major à adopter une ligne de conduite, puis exploiter cet état d'esprit au moyen d'une opération de déception. Les OI peuvent souvent se dérouler dans des conditions de dégradation. Outre les actions de l'adversaire ou les accidents, les phénomènes naturels peuvent causer une dégradation ou une perturbation du matériel ou des services. En raison de la complexité et de la fragilité des SIC, les plans d'une unité devraient inclure des procédures en vue de l'utilisation des SIC dans des conditions de dégradation.

EMPÊCHER

51. Les OI offensives rendent possible l'attaque d'un adversaire simultanément à tous les niveaux avec une force écrasante. Les OI offensives visent à empêcher un adversaire d'exercer un commandement et un contrôle efficaces et de maintenir la cohésion de ses forces en l'empêchant de disposer d'information, ou en influençant, dégradant ou détruisant son information et ses SIC.

52. Les OI donnent au commandant les moyens d'attaquer un adversaire sur toute la profondeur de la zone d'opérations, loin au-delà de la portée des systèmes de tir directs ou indirects. Le but est de diminuer la confiance de l'adversaire dans ses données ou dans sa capacité de commander et de contrôler les opérations. En attaquant ou brouillant le sens du champ de bataille de l'adversaire, les forces amies s'assurent de la supériorité de l'information, et gagnent un avantage relatif subséquent en appliquant la puissance de combat ou en contrôlant la situation. L'utilisation des OI offensives pour parvenir à la supériorité de l'information est critique au soutien de notre approche manoeuvriste en matière d'opérations.

53. L'interdiction de l'accès à l'information exige généralement du temps et porte sur des zones relativement grandes. Pour rendre un adversaire aveugle ou sourd, il faut que la majeure partie de ses systèmes ISTAR importants soient sous l'influence des forces amies ou fassent l'objet d'interceptions par ces dernières. Les attaques contre les SIC adversaires sont donc normalement planifiées comme une série d'engagements dans le cadre d'une opération plus large ou d'un objectif plus important.

54. Les niveaux de commandement ne disposent pas tous des ressources nécessaires pour s'acquitter de la totalité des missions d'OI offensives, en particulier les opérations de déception et les OPSPSY. Les efforts de neutralisation de l'efficacité du commandement d'un adversaire et d'influence sur la perception de ses troupes et de la population dans la zone d'opérations ont toutefois une valeur importante, et les commandants à tous les niveaux doivent être préparés à contribuer à l'atteinte de ces buts. L'analyse et l'évaluation des objectifs possibles mèneront à des options d'attaque multiples, en matière d'OI. De manière générale, plus tôt le cycle de prise de décisions d'un adversaire sera interrompu, plus l'effet sur son potentiel sera grand. Il est souvent plus efficace d'interrompre les processus initiaux d'estimation ou de prise de décisions d'un adversaire que de tenter d'interrompre l'exécution d'une décision déjà prise. Les commandants opérationnels doivent évaluer les avantages d'une attaque des nœuds de commandement et de contrôle de l'adversaire par rapport à la perte possible de renseignement en provenance des signatures, rayonnements ou émissions de l'adversaire, et à la nécessité de protéger les méthodes et sources de renseignement.

SECTION 5
INTERACTION AVEC D'AUTRES FONCTIONS DE COMBAT

COMMANDEMENT

55. Les OI soutiennent directement la fonction de commandement. Les OI fournissent l'information nécessaire au cycle de décision-action du commandant et coordonnent tous les aspects de l'information. La nature même des OI est d'aider le commandant à vaincre un adversaire en préservant son propre cycle de décision-action tout en réduisant la capacité de l'adversaire à parvenir à la supériorité de l'information. Les OI seules peuvent permettre à un commandant de vaincre un adversaire ou l'empêcher de parvenir à la victoire.

PROTECTION

56. Les OI défensives contribuent manifestement de façon importante à la protection et doivent de ce fait être intégrées au processus de planification. Dans le contexte des OI, la protection signifie la protection de l'information, des processus, des systèmes et des sources de manière à assurer la liberté d'action d'un commandant. Les OI défensives prennent plusieurs formes, comme la protection électronique des systèmes d'information, la protection des sources d'information, et la protection physique tant du matériel que du personnel, en particulier les commandants. L'importance de la protection nécessaire dépend du potentiel des systèmes ISTAR de l'adversaire de collecter et d'exploiter notre information. Il faut comprendre que l'information ne peut pas toute être protégée contre un adversaire déterminé. Une appréciation renseignement des points faibles des forces amies joue un rôle clé dans la mise en place d'une protection suffisante qui ne nuise pas à la souplesse d'un commandant. Les OI défensives doivent être intégrées au plan de protection d'ensemble par des spécialistes des OI conformément au chapitre 6 de la B-GL-300-006/FP-001, *Protection de la Force terrestre*.

PUISSANCE DE FEU

57. Tous les types de puissance de feu dépendent de la qualité et de l'opportunité de l'information de sélection des objectifs. Les OI fournissent les capteurs, l'analyse et le flux d'information nécessaires à l'engagement d'un objectif, et déterminent le degré de réussite de l'engagement. Les objectifs doivent maintenant être envisagés non seulement du point de vue du matériel, mais également des processus, des interactions humaines (comme la cohésion du moral) et des effets temporaires. Le processus de sélection d'objectif fait le lien entre les OI (et leurs éléments comme les systèmes ISTAR et la guerre de commandement et de contrôle (GCC)) et la puissance de feu. Les OI offensives doivent être intégrées au processus de sélection d'objectif. Le spécialiste des OI peut désigner les objectifs, mais il appartient au commandant de décider de la priorité des efforts et de l'allocation des ressources. Le processus de sélection d'objectif est discuté plus en détail au chapitre 4 de la B-GL-300-007/FP-001, *Puissance de feu de la Force terrestre*.

MANOEUVRE

58. Les OI déterminent les points faibles et fournissent l'information au commandant de manière que les forces appropriées puissent intervenir au bon endroit au bon moment. Les OI fournissent la capacité de perception de la situation dont un commandant a besoin pour combattre et planifier les opérations futures.

MAINTIEN EN PUISSANCE

59. L'information est critique au maintien en puissance des forces. La SA et la visibilité des ressources sont critiques au réapprovisionnement « juste en temps » de l'ensemble des unités d'une formation. Les troupes de maintien en puissance ont besoin de types spécifiques de bases de données et d'un accès aux stocks nationaux pour prévoir les niveaux de maintien en puissance. Les systèmes d'information devront être robustes et bénéficier de protection. Comme le maintien en puissance doit s'étendre du théâtre d'opération au niveau national/stratégique, il est extrêmement vulnérable aux perturbations dues aux OI.

CHAPITRE 3
SYSTÈMES D'INFORMATION ET DE COMMUNICATION

Définition-Ensemble de matériels, de méthodes et de procédures et, le cas échéant de personnes, organisé de façon à accomplir des fonctions déterminées de transport et de traitement d'informations.

(Déf. OTAN AcomP-1, oct. 94)

SECTION 1
L'ENVIRONNEMENT

1. L'évolution rapide des technologies basées sur l'information et un environnement global de plus en plus compétitif ont placé l'information à l'avant-scène de la société, du gouvernement et de la conduite de la guerre. Toutes les révolutions technologiques du présent siècle manquent d'éclat lorsqu'on les compare aux progrès spectaculaires survenus dans le domaine de l'électronique des semi-conducteurs au cours des trois dernières décennies – des progrès sans pareil dans l'histoire de l'humanité. La puce électronique a généré une révolution phénoménale dans le domaine de l'information. Le stockage et le traitement de l'information, ainsi que les technologies basées sur l'information, ont une importance prépondérante et exercent une incidence sur tous les aspects de la guerre : de la planification au déploiement et au processus de maintien de la puissance, jusqu'à la surabondance de systèmes d'armes utilisés par les forces terrestres, aériennes et maritimes.

2. Cet usage accru entraîne une dépendance, comme l'illustre le tableau de la Figure 3-1-1. La courbe d'augmentation du flux et de la vitesse de traitement de l'information au XX^{e} siècle est presque verticale. L'information exacte et pertinente est absolument essentielle auux opérations militaires, alors que les structures de force importantes sont remplacées par des forces plus petites, hautement spécialisées et équipées d'un matériel techniquement avancé.

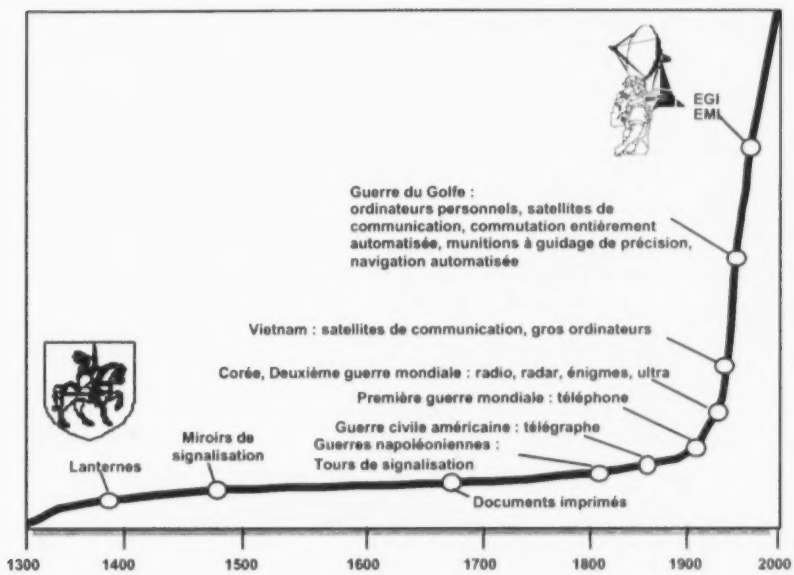

Figure 3-1-1 : Vitesse croissante du flux et du traitement de l'information au cours des âges

3. L'information elle-même est une ressource globale, vitale à la sécurité nationale. Des systèmes d'information de plus en plus complexes sont intégrés à des disciplines traditionnelles comme la mobilité, la logistique, la puissance de feu et les communications. Ces systèmes comportent une vulnérabilité inhérente qui, dans de nombreux cas, est la conséquence inévitable d'une fonctionnalité, d'une efficacité et d'une commodité d'utilisation accrues. Le coût relativement faible de ces technologies en fait une façon efficiente et rentable d'accroître le potentiel (et la vulnérabilité) d'un nombre sans précédent d'utilisateurs. L'accessibilité et l'emploi généralisé de ces systèmes d'information améliorent la conduite de la guerre. Leurs capacités mènent toutefois à une dépendance, laquelle crée la vulnérabilité. Cette vulnérabilité est une arme à double tranchant – constituée d'un côté par les secteurs que la Force terrestre doit protéger, et de l'autre par les faiblesses qu'elle peut exploiter chez l'adversaire.

SECTION 2
FONCTIONS

4. Le système d'information et de communication (SIC) de la Force terrestre soutient les opérations en fournissant le réseau d'information

numérique intégré dont le commandant a besoin pour parvenir à la supériorité de l'information sur le champ de bataille. Ces systèmes soutiennent les processus d'état-major et permettent un partage général de l'information, favorisant la compréhension mutuelle et l'unité de l'effort. La Force terrestre doit être capable de fonctionner en tant qu'élément d'une force interarmées multinationale et a besoin d'un SIC doté d'une interopérabilité élevée. Le système de la Force terrestre doit également procurer une connectivité fiable aux forces en campagne et à l'infrastructure, y compris des interfaces avec les forces amies et une infrastructure permettant l'acquisition, le traitement et la diffusion de l'information nécessaire au succès de la mission du commandant. Une interopérabilité fonctionnelle complémentaire est également nécessaire entre les plates-formes des systèmes de détection, les réseaux de communication et les systèmes d'information connexes. Pour assurer le degré requis d'interopérabilité, la Force terrestre doit établir un contrôle architectural en définissant les exigences et les normes techniques d'interopérabilité, ainsi que les lignes directrices en matière d'intégration des systèmes.

5. La fonctionnalité et les niveaux d'interopérabilité requis seront atteints au moyen de technologies existantes et nouvelles. Les technologies numériques permettent de mieux exploiter l'information, et procure de ce fait l'avantage de l'information sur le champ de bataille. Les technologies numériques sont appliquées au soutien de l'acquisition (p. ex., les systèmes de détection), de la diffusion (p. ex., les communications) et du traitement (p. ex., les systèmes d'information) de l'information. Les autres technologies qui assurer une fonctionnalité accrue incluent les techniques de compression des données, les technologies de réseau avancées et les concepts de sécurité à niveaux multiples. Ces technologies sont intégrées de manière à doter la Force terrestre d'un réseau numérique décloisonné et interopérable qui s'étend aux diverses fonctions tant sur le champ de bataille que dans les bases, et ce, jusqu'au niveau stratégique national. Le rythme rapide des progrès en matière de technologie de l'information est ralenti par les réalités et priorités financières de la Force terrestre. Ceci signifie que la Force terrestre doit avoir recours à un processus d'acquisition progressive de ces technologies et capacités, prendre avantage des progrès des forces alliées, et utiliser des technologies et produits commerciaux, gouvernementaux et militaires courants.

6. Ce processus d'acquisition progressive, s'il satisfait aux réalités et priorités financières de la Force terrestre, pourrait mener à une asymétrie des capacités qui devra être prise en compte dans toute évaluation du potentiel. De même, la Force terrestre doit supposer, dans

tout déploiement ou toute action, que les adversaires peuvent disposer d'au moins certains types d'arme de pointe, même si cette arme n'est simplement qu'un ordinateur relié à Internet. L'adversaire pourrait également disposer de technologies de l'information ou capacités, dans des créneaux spécifiques, qui poseront un défi asymétrique pour la Force terrestre.

SECTION 3
RÔLE

7. Le rôle des SIC est de fournir l'infrastructure permettant à la Force terrestre d'opérer à l'intérieur de l'EMI et d'établir une interfacer avec l'EGI. Les SIC facilitent l'intégration de l'ensemble des activités. Les principaux rôles des SIC sont de :

a. soutenir le processus de prise de décisions;

b. transmettre l'information, dont les ordres et rapports;

c. relier les capteurs, commandants et tireurs;

d. fournir une image multidimensionnelle pertinente commune;

e. assurer un maintien en puissance efficace de la force.

8. L'évolution accélérée des technologies de l'information a créé de nouvelles techniques de gestion, de transport, de traitement et de présentation des données. Ces techniques incluent l'imagerie numérique, la vidéo, les graphiques couleurs, les fonds de page numériques, l'information géospatiale et les bases de données. La révolution des technologies de l'information, les progrès en matière de communications par satellite, de réseaux et d'ordinateurs, ainsi que les percées dans des secteurs complémentaires de nature non militaire, donnent au commandant la possibilité de disposer d'une couverture globale. L'architecture des SIC doit permettre l'utilisation d'une force sur mesure au cours de toutes les phases d'opération. Les opérations prennent place dans un environnement global, ce qui suppose que l'information provient d'une variété de sources. Les systèmes militaires et non militaires fournissent cette capacité globale et appuient les commandants dans l'ensemble des opérations possibles (voir la Figure 3-3-2). La Figure 3-3-2 constitue la structure représentative combinant les systèmes militaires/commerciaux canadiens et les systèmes militaires alliés.

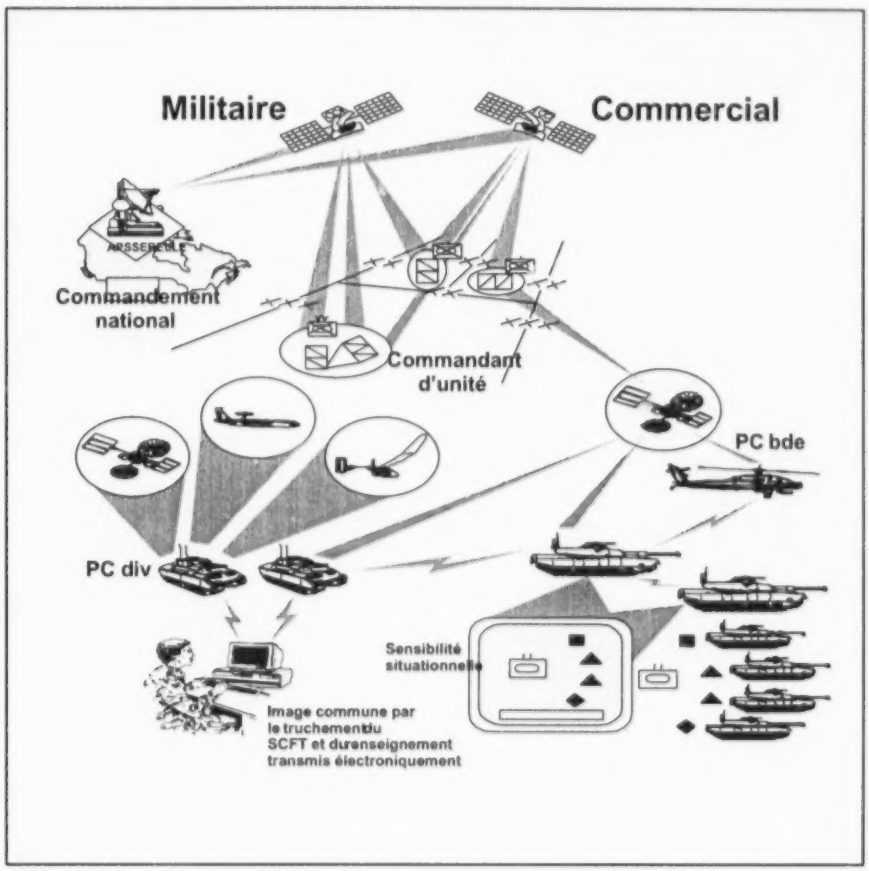

Figure 3-3-2 : Réseau de communications globales

SECTION 4
SYSTÈMES MILITAIRES

9. Les SIC intègrent les communications et les systèmes automatisés militaires de manière à relier les quartiers généraux stratégiques, opérationnels et tactiques. Les SIC maximisent la disponibilité des réseaux d'information grâce à une connectivité et une interopérabilité presque totales.

10. Le SICCFT se définit comme étant « *l'ensemble informatisé incluant les doctrines, les procédures, les organisations, le personnel, les équipements, les moyens divers et les liaisons, destiné à fournir en temps opportun aux autorités à tous niveaux les informations correctes dont elles ont besoin pour la planification, la direction et le contrôle de leurs tâches* ». Dans son sens le plus large, ce système englobe : la gestion de

l'information (GI), qui constitue l'aspect ligne de conduite, planification et stratégie, les systèmes d'information (SI), qui sont l'aspect procédures et, enfin, le matériel. Le matériel comporte à son tour deux éléments, soit le matériel non automatisé, comme les dossiers et livres, et la technologie de l'information, qui est la portion automatisée du matériel, et est constituée des applications, de l'infrastructure et des bases de données.

11. L'architecture du Système d'information, de commandement et de contrôle de la Force terrestre (SICCFT) appuie le système de commandement et de contrôle de la Force terrestre (SCCFT). Cette architecture est fondée sur une interopérabilité à trois niveaux (voir la Figure 3-4-3). Les différents systèmes d'information sont intégrés en un noyau central commun servant aux opérations tant dans les bases que sur le terrain. Ce noyau assure également l'interopérabilité des forces interarmées et multinationales. Le tiers inférieur de l'architecture est en quelque sorte la base sur laquelle repose le reste de la stratégie, et se compose du réseau principal de diffusion d'information numérique, et de la capacité de positionnement et de navigation. Le tiers intermédiaire est le noyau central, qui fournit les applications et services communs comme les outils de commandement et de contrôle, les services géospatiaux numériques, la gestion des bases de données, la planification, la préparation des ordres et les transmissions. Ce noyau central est adapté aux besoins des utilisateurs. Le tiers supérieur est constitué des applications spécialisées et fonctionnelles qui complètent la fonctionnalité du noyau central. Ces dernières sont des applications et non pas des systèmes autonomes, car elles utilisent le noyau central pour leur fonctionnalité de base.

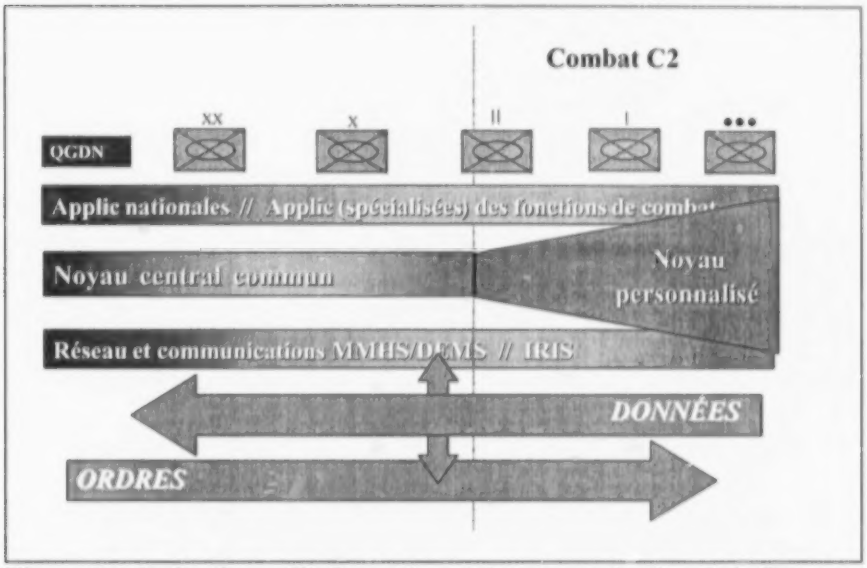

Figure 3-4-3 : Systèmes d'information et de communication de la Force terrestre

SECTION 5
SYSTÈMES D'INFORMATION NON MILITAIRES

12. La technologie de l'information connaît une croissance exponentielle et transforme la façon de faire des affaires, d'entretenir des relations diplomatiques et de faire la guerre partout dans le monde. Ceci signifie que les commandants doivent avoir une vue beaucoup plus large des sources d'information lorsqu'ils exécutent des opérations d'information (OI). Le dilemme est que la Force terrestre possède un pouvoir limité en matière d'utilisation de l'infrastructure civile ou d'influence sur le contenu des produits de cette infrastructure. Les améliorations technologiques en mobilité, numérisation, armes et capteurs continuent à réduire les facteurs temps et espace, et exigent un rythme de déroulement des opérations plus rapide réparties sur des territoires beaucoup plus grands.

13. La population mondiale croissante, les marchés économiques mondiaux en expansion rapide et les percées sans précédent en matière de technologie des systèmes d'information créent une explosion mondiale de réseaux d'information non militaires ou commerciaux. Ces réseaux en expansion continue mènent rapidement à la création d'un réseau mondial ou infosphère. Le caractère mondial de l'information et la vitesse à laquelle cette information est transmise peuvent élever des nouvelles apparemment sans intérêt au rang de manchettes internationales. Le nombre en croissance rapide des intervenants dans l'EGI partage de

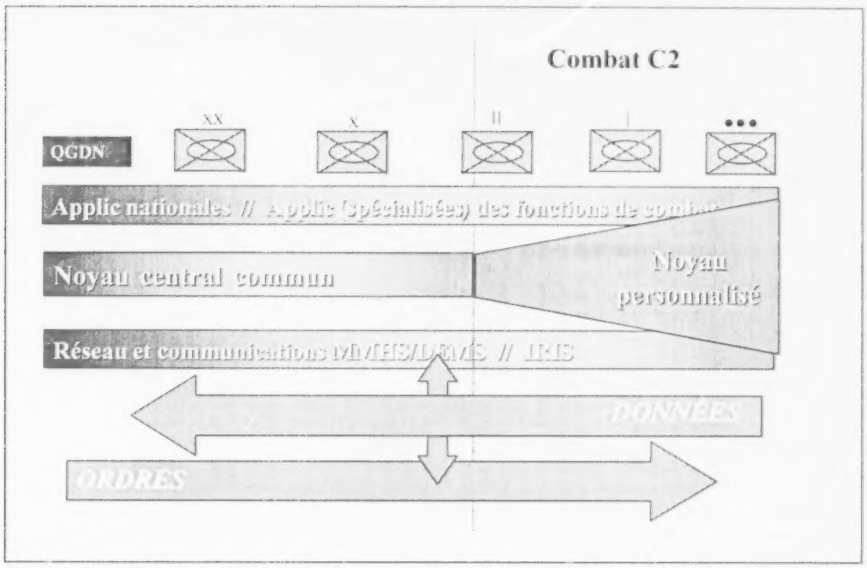

Figure 3-4-3 : Systèmes d'information et de communication de la Force terrestre

SECTION 5
SYSTÈMES D'INFORMATION NON MILITAIRES

12. La technologie de l'information connaît une croissance exponentielle et transforme la façon de faire des affaires, d'entretenir des relations diplomatiques et de faire la guerre partout dans le monde. Ceci signifie que les commandants doivent avoir une vue beaucoup plus large des sources d'information lorsqu'ils exécutent des opérations d'information (OI). Le dilemme est que la Force terrestre possède un pouvoir limité en matière d'utilisation de l'infrastructure civile ou d'influence sur le contenu des produits de cette infrastructure. Les améliorations technologiques en mobilité, numérisation, armes et capteurs continuent à réduire les facteurs temps et espace, et exigent un rythme de déroulement des opérations plus rapide réparties sur des territoires beaucoup plus grands.

13. La population mondiale croissante, les marchés économiques mondiaux en expansion rapide et les percées sans précédent en matière de technologie des systèmes d'information créent une explosion mondiale de réseaux d'information non militaires ou commerciaux. Ces réseaux en expansion continue mènent rapidement à la création d'un réseau mondial ou infosphère. Le caractère mondial de l'information et la vitesse à laquelle cette information est transmise peuvent élever des nouvelles apparemment sans intérêt au rang de manchettes internationales. Le nombre en croissance rapide des intervenants dans l'EGI partage de

l'information nouvelle sur des réseaux à une vitesse en augmentation continue.

14. Les communications cellulaires et les progrès en matière de compression de données procurent une liberté de communication de plus en plus grande aux individus dans des régions de plus en plus étendues du globe. Ces progrès permettent aux soldats, ainsi qu'aux médias et à d'autres intervenants, de communiquer de façon autonome au moyen d'Internet ou de sources de diffusion ou de publication. Les sources possibles d'information immédiate, et le nombre et la variété des influences exercées sur l'EMI (tant volontaires qu'involontaires) se multiplient rapidement. Les effets cumulatifs de ces changements modifient en permanence la forme des organisations et les architectures des SICC d'une façon qui devient apparente seulement maintenant.

15. Une bonne partie du flux d'information de la Force terrestre utilise des systèmes commerciaux. Ceci est très vrai sur le plan intérieur, et, comme la plupart des pays, la Force terrestre compte sur des éléments d'un environnement de l'information sur lequel elle n'a pas d'emprise. Les exemples de systèmes d'information non militaires incluent notamment :

a. les réseaux commutés publics, les réseaux postaux et les réseaux télégraphiques canadiens et des pays hôtes;

b. les satellites commerciaux de communications comme INTELSAT et INMARSAT;

c. les médias d'information commerciaux et internationaux;

d. les bases de données et babillards électroniques à accès public.

16. Si la disponibilité des systèmes d'information non militaires peut souvent offrir aux commandants une façon autre de satisfaire à des besoins, les risques de sécurité de cette option doivent être évalués avec soin. L'utilisation de systèmes d'information non militaires peut également réduire le nombre de systèmes d'information militaires requis, et permettre aux planificateurs de solutionner les problèmes de pénurie ou de satisfaire à des besoins de pointe dans la région concernée. De plus, l'utilisation de systèmes d'information non militaires peut permettre des économies sur le plan du soutien et de la maintenance.

SECTION 6
PLANIFICATION DES COMMUNICATIONS ET DES SYSTÈMES D'INFORMATION

SYSTÈMES D'INFORMATION NON MILITAIRES

17. Le G6 est responsable de la normalisation du matériel et des logiciels non militaires utilisés dans l'ensemble de la zone d'opérations. Les planificateurs qui prévoient l'utilisation de systèmes d'information modulaires deoivent s'assurer que ces systèmes sont de préférence ouverts, et font appel à des normes et protocoles normalisés, de manière à simplifier les exigences d'interface.

INSTRUCTION

18. Les utilisateurs doivent affronter le défi posé par la numérisation du champ de bataille, par les exigences d'interface entre les opérateurs et le système, et par la nécessité d'élaborer des stratégies d'instruction efficaces. L'usage optimal des systèmes d'information dépend de la disponibilité de soldats de qualité et de chefs formés à l'utilisation des technologies de l'information de pointe. Les organisations doivent élaborer des stratégies organisées de tâches souples fondées sur l'utilisation des systèmes d'information, pour s'adapter au large éventail de conditions qui existent dans l'EGI. Des défis majeurs se posent du point de vue tant de l'instruction que de l'organisation. Ces défis sont les suivants :

a. une technologie en évolution constante;

b. une distribution / mise en service inégales du matériel ou de la capacité;

c. la recherche et l'utilisation de produits disponibles dans le commerce.

SOUTIEN DES COMMUNICATIONS

19. Tous les aspects des OI ont grand besoin du soutien des communications pour l'acheminement de l'information, non seulement dans la zone d'opérations, mais également entre le niveau national ou le théâtre et la zone d'opérations. Ce soutien requiert la participation de nombreux systèmes et de tous les types de communications, à partir des passerelles stratégiques jusqu'aux éléments avancés les plus déployés

d'une force. Les besoins de soutien en matière de communications sont énormes, varient considérablement et requièrent une flexibilité maximale.

20. Le SIC doit être adaptable et doit répondre aux besoins des commandants, et inclure les caractéristiques suivantes :

a. numérisation et compression de l'information tactique multimédia au moyen de systèmes de transport à largeur de bande accrue et haute efficacité;

b. encodage et niveaux de protection requis dans tous les secteurs;

c. gestion des réseaux d'information au moyen de procédures et de logiciels intelligents qui optimisent la capacité et le débit, et assurent la diffusion et la redondance;

d. affichage de l'image commune pertinente de la situation à l'intention des commandants.

CAPACITÉS

21. Pour que les utilisateurs puissent mener des opérations efficaces partout sur le champ de bataille, les fonctions de transfert et le traitement de l'information doivent être protégées, continues et avoir une grande capacité. Ces fonctions doivent ultimement inclure les opérations multimédias, c.-à-d. le transport des signaux vidéos, desimages, des données et des sons. Ceci permet au commandant de visualiser l'état tant actuel que final souhaité de la bataille et du champ de bataille. Certaines des fonctions de base du système de communication doivent inclure :

a. un lien entre la force et l'EMI/EGI de manière à assurer une connectivité complète tant sur le champ de bataille que dans les bases;

b. des communications hiérarchiques haute capacité;

c. la diffusion de l'information non hiérarchique à large bande;

d. l'exécution d'opérations à partir de bases différentes décloisonnées communiquant avec des plates-formes et centres de fusion de l'information divers par l'intermédiaire de points d'entrée stratégiques.

TECHNOLOGIE FUTURE

22. Le rythme et l'étendue du changement technologique sont un des plus grand défis des OI. Les percées en matière de technologie de l'information permettent aux commandants de se faire une image plus complète du champ de bataille, de prendre rapidement de meilleures décisions, d'effectuer des manœuvres plus rapides, et d'augmenter la souplesse et l'agilité des unités. La technologie est n'est qu'un outil et ne remplace pas les chefs bien formés et les organisations tactiques efficaces. Certains des possibilités et domaines futurs incluront :

a. Une capacité tactique Internet permettant le partage de l'information et des communications directes entre à peu près tous les utilisateurs, et menant à un niveau entièrement nouveau d'intégration, de coordination et de synchronisation non hiérarchiques qui coexisterait avec le système vertical actuel.

b. L'utilisation de technologies de compression et de transmission d'image assurant le transfert des images et des signaux vidéos en provenance de divers capteurs et plates-formes, et permettant une meilleure compréhension de la zone d'opérations aux fins de la planification, de la préparation et de l'exécution des missions.

c. L'utilisation du multimédia permettra une présentation tridimensionnelle de l'imagerie et des graphiques grâce à laquelle les commandants pourront visualiser leur zone d'opérations beaucoup plus efficacement.

SÉCURITÉ

23. La sécurité est à la fois un des plus grands défis et un des aspects les plus vulnérables. La dépendance croissante vis-à-vis des SI a créé une capacité accrue en même temps qu'une plus grande vulnérabilité. Les systèmes et réseaux d'ordinateurs, sur lesquels dépendent presque tous les aspects de l'administration, du soutien et des opérations, sont vulnérables en tout temps aux attaques. Ainsi, la société américaine Rand affirme que l'anonymité du cyberespace a brouillé la distinction entre criminalité et guerre, entre accidents et attaques. Un large éventail de méthodes et de techniques, dont certaines sont énumérées ci-dessous, peuvent servir à accéder à un réseau d'ordinateurs ou de communications :

a. insertion d'un logiciel nuisibles par l'entremise d'entrepreneurs;

b. monitorage des modifications logicielles et des activités d'exploitation du système;

c. modification des chemins d'accès ou utilisation de dispositifs « renifleurs » qui captent l'information pendant les communications et les mots de passe.

24. Ces intrusions peuvent être effectuées en tout temps ou en tout point d'une opération. De même, les mesures et procédures de sécurité doivent préserver, tant activement que passivement, la confidentialité, l'intégrité et la fonctionnalité du SI. Les exigences de protection incluent la mise en œuvre de mesures en temps quasi-réel qui détectent les points vulnérables, les altérations et les intrusions, et neutralisent ces risques en restaurant le SI. Exemples de mesures de détection possibles :

a. procédures d'assurance de la qualité;

b. équipes de repérage des points vulnérables des réseaux et des communications;

c. blocage de tout accès non autorisé;

d. renforcement des programmes.

25. La grande majorité des intrusions est attribuable à l'erreur humaine. L'instruction et la conformité à la sécurité opérationnelle (SECOP) des gestionnaires de système, opérateurs et utilisateurs sont les meilleures mesures de lutte contre l'atteinte à l'intégrité des systèmes. En outre, les gestionnaires de système doivent être capables de dépister les intrus.

26. Outre le dépistage des intrus, les programmes doivent être renforcés contre les tentatives d'accès à l'information ou d'endommagement du flux d'information. Aucun plan de protection n'est parfait, et les ressources de protection/restauration sont limitées. Les plans et ordres doivent en conséquence spécifier le niveau de priorité de l'effort de protection.

GESTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATIONS

27. Un autre aspect critique est celui de la gestion de ces systèmes. En raison des limitations de l'environnement des communications (ressources et technologie), une bonne stratégie de gestion des SI qui

établisse l'ordre de priorité de l'information est requise. Les commandants à tous les niveaux doivent définir avec soin leurs besoins essentiels d'information. On ne doit pas oublier que le but des SI automatisés est de parvenir à un avantage informationnel en utilisant et gérant l'information nécessaire à une prise de décisions opportune et appropriée dans toutes les opérations. Le but de l'état-major est de tirer avantage de la technologie disponible en utilisant un SI qui procure au commandant l'information souhaitée au bon moment et au bon endroit.

28. Toute l'information fournie par l'état-major est fondée sur l'intention du commandant, son concept des opérations et les BECI. Les BECI définissent les besoins d'information du commandant, axant ainsi l'action de l'état-major et le soutien informationnel sur l'acquisition, la fusion et l'analyse rapides de l'information. Les SI complètent les rapports d'acheminement ou périodiques en fournissant de l'information spécifique.

29. Les activités et exigences applicables incluent notamment :

a. la planification du réseau de systèmes d'information (y compris les échanges d'information, l'emplacement des bases de données et la reproduction de l'information);

b. la planification de la connectivité des communications;

c. la planification de la sécurité du réseau;

d. l'allocation des fréquences (y compris une gestion efficace du spectre par le G6 au soutien de tous les aspects des OI et types d'OI);

e. le contrôle et la supervision de la connexion des systèmes;

f. la reconfiguration du réseau en fonction des besoins;

g. le maintien et la mesure de la performance du réseau;

h. la planification de la dégradation du réseau;

i. la mise en application de la continuité des plans opérationnels en fonction des besoins.

CHAPITRE 4
INFORMATION PERTINENTE

Dans la conduite moderne de la guerre, l'importance de l'information disponible pose des défis aux chefs à tous les niveaux. En bout de ligne, ils doivent assimiler des milliers de bits d'information pour visualiser le champ de bataille, évaluer la situation et orienter l'action militaire requise pour parvenir à la victoire.

Armée américaine

SECTION 1
INTRODUCTION

1. Le présent chapitre définit le fondement doctrinal du rôle de l'information pertinente, laquelle inclut le renseignement (voir la figure 4-2-1). Le chapitre examine la nécessité de l'information pertinente, les critères qui permettent une évaluation attentive de cette information et le cycle de décision-action du commandant. Il inclut également de l'information sur le rôle du renseignement dans l'acquisition de l'information pertinente sur les ennemis.

SECTION 2
INFORMATION PERTINENTE

2. Par information pertinente, on entend l'information tirée de l'environnement militaire de l'information (EMI) dont l'incidence, la contribution ou le lien avec l'exécution de la mission considérée ont une importance significative.

3. L'information pertinente a un lien direct avec l'EMI de deux façons importantes :

a. en premier lieu, l'action de recueillir, traiter ou diffuser l'information pertinente est le principal critère sur lequel un commandant se base pour inclure un individu, une organisation ou un système dans l'EMI;

b. elle est le produit ou le moyen, obtenu de ces intervenants ou utilisé par eux, qui sert de base aux Opérations d'information (OI).

4. Dans le passé, l'Armée de terre a eu tendance à considérer la collecte et l'utilisation de l'information opérationnelle d'un point de vue spécialisé. Par exemple, différentes sous-fonctions recueillaient et utilisaient l'information nécessaire au soutien de leurs propres fonctions :

a. le renseignement visait l'information relative à l'adversaire et aux pays étrangers;

b. les opérations visait l'information situationnelle touchant les forces amies;

c. la logistique s'intéressait aux conditions et besoins relatifs au maintien en puissance de la force amie;

d. les Affaires publiques (AP) et la Coopération civilo-militaire (COCIM) faisaient porter leurs efforts sur l'interface entre les secteurs militaire et non militaire.

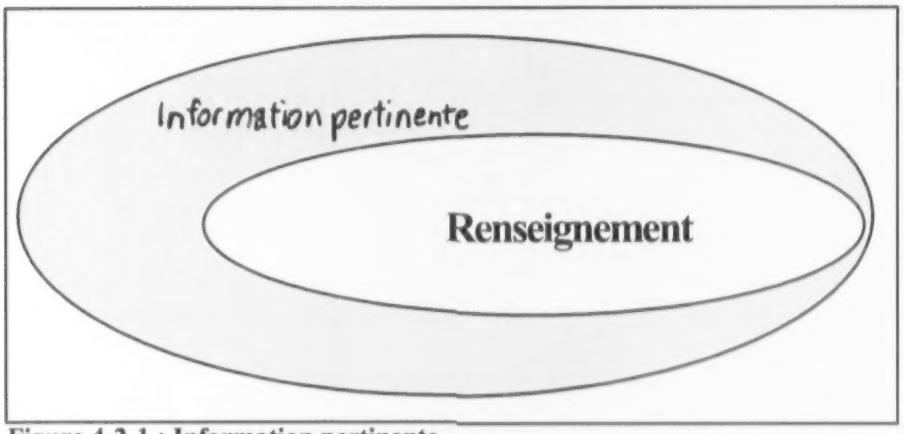

Figure 4-2-1 : Information pertinente

5. En raison des changements survenus dans les environnements informationnels et opérationnels, nous pouvons maintenant atteindre des niveaux d'efficience et d'efficacité novateurs dans l'utilisation de l'information en intégrant et coordonnant les efforts de collecte, de traitement et de diffusion. Ces efforts doivent chercher à tirer avantage de la contribution opérationnelle possible de l'information en recueillant celle-ci et en la diffusant à tous les éléments avec efficience.

SECTION 3
CRITÈRES D'ÉVALUATION

6. Comme les sources d'information sont imparfaites, et sont susceptibles de distortion et de déception, les commandants et les planificateurs doivent évaluer avec soin la qualité de l'information avant de l'utiliser. Ils peuvent le faire en appliquant les six critères suivants :

a. **Exactitude.** L'information dépeint la situation véritable.

b. **Pertinence.** L'information s'applique à la mission, la tâche ou la situation en cause.

c. **Opportunité.** L'information est disponible en temps opportun pour la prise de décisions.

d. **Forme utilisable.** L'information est présentée sous une forme normalisée et facile à comprendre.

e. **Complétude.** L'information contient tous les renseignements nécessaires requis par le décideur..

f. **Précision.** L'information présente le niveau requis de détail.

7. L'information doit avant toute chose être exacte et pertinente. En deuxième lieu, elle devrait être à la fois opportune et fournie sous une forme utilisable. Enfin, l'information devrait être aussi complète et précise que possible. La règle empirique qui suit établit les liens que voici entre ces différents critères :

a. de l'information incomplète ou imprécise est meilleure qu'une absence totale d'information,

b. de l'information non opportune ou inutilisable n'a pas plus de valeur qu'une absence totale d'information,

c. de l'information inexacte ou non pertinente est pire qu'une absence totale d'information.

8. Les commandants doivent disposer d'information pour commander. L'information est le moyen qui permet au cycle décision-action du commandant d'être efficace. L'information donne une orientation aux actions de la force, et fournit des plans d'action qui protègent cette dernière et l'aident à accomplir sa mission. L'information pertinente tirée de l'EMI favorise l'acquisition de la capacité de perception de la situation qui contribue directement à un commandement

efficace au cours de l'ensemble des étapes du cycle de décision-action. Une capacité de perception de la situation approfondie aide le commandant à assurer l'unité des efforts en vue de l'accomplissement de la mission. Ultimement, un commandement efficace repose sur le fait que la bonne personne dispose de la bonne information au bon moment.

9. Les commandants recueillent l'information, visualisent le champ de bataille, et planifient les opérations futures en même temps qu'ils conduisent les opérations en cours. Pendant ce temps, les commandants supérieurs et subordonnés recueillent l'information et mettent en œuvre les cycles de décision-action à leurs niveaux respectifs. Le maintien de cycles de décision-action rapides, et du rythme rapide des opérations qui en résulte, requiert que tant les supérieurs que les subordonnés possèdent une image exacte et commune de la zone d'opérations. À partir de cette image commune, une unité acquiert une plus grande capacité de perception de la situation lui permettant de faire preuve d'initiative au cours du combat ou dans d'autres situations.

10. Le commandant opère dans le cadre de l'environnement global de l'information (EGI), rajustant son EMI de manière à améliorer sa capacité de perception de la situation en fonction des besoins. De plus, le commandant utilise les divers moyens à sa disposition dans l'EMI pour assurer que tous les éléments de sa force partagent une image multidimensionnelle commune, complète et pertinente. Ceci requiert un système d'information et de communications (SIC) perfectionné qui améliore la capacité du commandant à partager, gérer et faire circuler l'information entre les organisations. Le commandant utilise également ses capacités informationnelles pour soutenir les opérations autres que la guerre. Pendant des opérations autres que les combats, l'accent passe des opérations de combat à des opérations autres que les combats, et inclut des considérations plus larges contribuant à l'efficience et à l'efficacité des opérations. Ces dernières font souvent intervenir une diversité d'acteurs de l'EGI. Par exemple, le G3 travaille en collaboration étroite avec les officiers des AP et de la COCIM, notamment pour déterminer les besoins essentiels en information relatifs à la zone d'opérations.

SECTION 4
RENSEIGNEMENT

Le renseignement est un terme utilisé pour décrire tant les activités d'acquisition et de traitement de l'information que le produit résultant de ce processus. Essentiellement, le renseignement consiste à recueillir de l'information et des connaissances, sur un

belligérant, au moyen de l'observation, de l'investigation, de l'analyse et de la compréhension.

Source inconnue

11. Le renseignement est le sous-élément des BBECI qui est axé principalement sur les pays étrangers, l'environnement et l'adversaire. Au soutien des opérations amies, le renseignement aide à produire une image commune, à jour et pertinente de la zone d'opérations, appelée capacité de perception de la situation, qui réduit l'incertitude et abrège le processus de prise de décisions du commandant. Dans le futur, les activités de renseignement seront conduites sur le principe des opérations partagées, ce qui permettra aux commandants tactiques de tirer profit des capteurs stratégiques et des capacités analytiques. Le soutien aux opérations dispensé par le renseignement aux niveaux stratégique et national doit être lié aux opérations de soutien conduites aux niveaux opérationnel et tactique. Cet effort requiert un processus de collecte de renseignement décloisonné, ainsi qu'une architecture de soutien de ce processus, et fournit des produits de renseignement en temps réel de prédiction axés sur les BECI, lesquels permettront à un commandant d'élaborer sa visualisation du champ de bataille (VCB).

RÔLE DU RENSEIGNEMENT

12. Le renseignement, y compris la contre-ingérence (CI), fournit au commandant une compréhension exacte de la situation de risque reliée aux opérations courantes et futures. Le personnel du renseignement acquiert, utilise, gère et exploite l'information de manière à parvenir à une compréhension de l'adversaire qui soit exacte et qui permette de faire des prédictions. Pour que la capacité de perception de la situation commune soit exacte et à jour, l'effort de renseignement doit être continu. La collecte du renseignement inclut toutes les sources possibles, des opérations nationales secrètes aux sources locales ouvertes comme les médias d'information, les contacts dans le monde des affaires et le monde universitaire, et les individus.

13. Dans les opérations autres que les combats , le renseignement humain (HUMINT), les sources ouvertes et les autres agences gouvernementales fournissent une information opportune qui vise à augmenter l'effort de collecte-renseignement plus traditionnel de l'unité, axé sur le combat. L'effort de renseignement fournit des données à jour et exactes sur le risque et l'acquisition d'objectif aux systèmes d'armes et aux capteurs de renseignement. L'efficacité de ces derniers est tributaire du mouvement rapide des données entre la personne qui collecte les

données, celle qui les traite, celle qui prend les décisions et celle qui tire. Le renseignement soutient les OI en se concentrant sur les Opérations d'information offensives et défensives.

FONCTIONS DE RENSEIGNEMENT

14. Le but premier du renseignement est de soutenir la prise de décisions opérationnelle sur la base d'une compréhension exacte de la situation. Le renseignement consiste essentiellement à recueillir, analyser, trier et présenter l'information demandée par le commandant dans le cadre d'activités de fourniture de renseignement à jour au soutien de la capacité de perception de la situation, et de matériels prédictifs au soutien de la visualisation du champ de bataille. Les fonctions de renseignement portent sur l'évaluation des points vulnérables des forces amies, sur la compréhension de l'adversaire, sur l'utilisation de l'analyse tactique graphique et sur l'évaluation des dommages au combat.

ÉVALUATION DES POINTS VULNÉRABLES DES FORCES AMIES – CONTRE-INGÉRENCE

15. La première étape essentielle, dans la protection du potentiel, consiste à déterminer les risques spécifiques et possibles au moyen d'une estimation de CI. Les risques possibles vont des actions directes ouvertes et secrètes de l'adversaire, par l'entremise de ses activités de renseignement, de surveillance, d'acquisition d'objectif et de reconnaissance (ISTAR), aux individus et organisations qui cherchent à exploiter les SIC militaires, et aux phénomènes naturels. Elles incluent une nouvelle famille de systèmes d'imagerie commerciale mondiale, de communications cellulaires et de positionnement qui fournissent conjointement ou séparément à un adversaire possible de l'information presque en temps réel sur les forces et les mouvements.

16. La nature fluide et poreuse de l'EMI fait qu'il est difficile de protéger les SIC contre les attaques possibles. Le renseignement fournit en conséquence au commandant l'information dont il a besoin pour effectuer une évaluation des risques et élaborer les options de gestion des risques qui lui permettront de protéger les composantes et capacités vitales de commandement et de contrôle. L'évaluation des risques est fondée sur la détermination de facteurs comme le potentiel de risque spécifique, le potentiel technique, la doctrine et les performances antérieures de la force qui présente un risque. L'évaluation des risques n'est pas un document fini, mais un processus continu constamment mis à jour en fonction des changements dans l'environnement opérationnel, la technologie et la

détermination des risques. Parce que les OI offrent aux adversaires possibles la chance de frapper l'infrastructure de soutien de la force – où que cette infrastructure soit située – le commandant et son état-major doivent être conscients des risques auxquels est exposé leur SIC à leur station de base.

COMPRÉHENSION DE L'ADVERSAIRE

17. L'efficacité des opérations offensives, y compris les OI, est fondée sur une compréhension en profondeur d'un adversaire, de son système de commandement et de contrôle, et de son processus de prise de décisions. Plus la compréhension sera approfondie, combinée à des outils et techniques permettant de prendre avantage de cette connaissance, plus l'exploitation de l'adversaire possible sera efficace. À tous les niveaux des opérations, le renseignement est un outil opérationnel qui identifie, évalue, et exploite les systèmes d'information et de commandement et de contrôle de l'ennemi. Des données sont en conséquence nécessaires sur l'information que l'adversaire recueille, les moyens qu'il utilise, le degré de fiabilité qu'il attribue aux différentes sources, et les méthodes dont il se sert pour évaluer l'information.

18. Le personnel du renseignement doit être en mesure de décrire le processus de prise de décisions de l'ennemi et comment les directives sont transmises aux subordonnés. Des renseignements détaillés sont nécessaires sur l'environnement social et culturel, ainsi que sur le profil psychologique des principaux chefs et décideurs de l'adversaire. Les interactions de ces derniers et la perception qu'ils ont les uns les autres sont des aspects importants de l'information nécessaire à l'élaboration d'opérations psychologiques (PSYOPS) et de déception efficaces. L'information sur la façon dont les subordonnés exécutent les décisions complète le tableau. Il est nécessaire d'avoir une compréhension détaillée de l'utilisation que l'adversaire fait de l'information pour déterminer sur quel point et comment influencer efficacement ses actions.

> *Connais l'ennemi et connais-toi toi-même et tu seras vainqueur.*
>
> Sun Tzu (500 av. J.-C.)

SECTION 5
UTILISATION DE L'ANALYSE TACTIQUE GRAPHIQUE

19. L'application de l'ATG dans le contexte des OI suit les étapes habituelles. L'étape 1 consiste à définir l'environnement du champ de

bataille et à évaluer l'EGI en ce qui a trait à la mission de la force. Une fois ces activités terminées, l'étape 2 de l'ATG consistera à décrire les effets du champ de bataille et à définir ainsi l'EMI, en mettant l'accent sur :

a. la connaissance des exigences techniques pour un large éventail de SIC;

b. la connaissance des influences politiques, sociales et culturelles à l'œuvre dans l'EMI;

c. la capacité d'exécution de processus hautement techniques visant à produire les modèles de plan d'action des OI;

d. la connaissance et une compréhension approfondie de la biographie et des antécédents des principaux chefs, décideurs, communicateurs et conseillers de l'adversaire.

20. Une bonne partie de cette information devrait avoir été recueillie de façon routinière et conservée dans des bases de données nationales, et être facilement disponible au début de la mission. Advenant qu'une opération soit ordonnée pour une zone d'opérations qui n'avait pas été prévue, toutefois, l'officier du renseignement devra exécuter les étapes de l'ATG à partir du début et avec de l'information brute.

21. Au cours de la troisième étape de l'ATG, le personnel du renseignement construit un modèle de la structure, de la doctrine, des tactiques, des techniques et des procédures de la force adversaire. Ce modèle nécessite une estimation du processus de prise de décisions de l'adversaire. Il est important de comprendre l'infrastructure informationnelle de l'adversaire, laquelle décrit comment l'information circule à l'intérieur de l'unité, de l'organisation et de la structure. Cette analyse inclut l'interface humaine en tant que forme valide de diffusion de l'information et n'est pas limitée aux évaluations purement technologiques. Cet aspect de l'ATG aide à comprendre les profils de leadership/personnalité des plus importants décideurs de l'adversaire. Il s'intéresse à la façon dont ces derniers utilisent l'information pour prendre des décisions, leurs interactions en tant qu'organisation en matière de prise de décisions, et comment ils mettent ces décisions en œuvre. Cette étape est directement liée à l'objectif ultime des OI, qui consiste à trouver des moyens de créer un état de supériorité de l'information dans la zone d'opérations.

22. Au cours de cette étape, l'officier du renseignement analyse le modèle de prise de décisions et le modèle d'infrastructure pour déterminer les points vulnérables de l'adversaire. L'analyse de la vulnérabilité s'effectue à deux niveaux :

a. les points vulnérables du système sont repérés et exploités de manière à produire les effets souhaités sur le processus de décision;

b. les points vulnérables matériels spécifiques du système sont déterminés.

23. L'analyse de la vulnérabilité est ensuite étendue au dommage collatéral que les activités des OI sont susceptibles de causer à l'environnement opérationnel. Par exemple, une des options envisagées, en matière d'attaque du système de commandement et de contrôle de l'adversaire, pourrait être la destruction de l'infrastructure de production d'électricité. Le coût stratégique (politique ou logistique) de la destruction de ce potentiel pourrait toutefois être supérieur aux gains tactiques obtenus. Une des implications de l'EGI est que les actions et leurs conséquences sont examinées pour l'ensemble de l'EMI, plutôt que par rapport au seul champ de bataille.

24. La compréhension de l'infrastructure informationnelle de l'adversaire, laquelle décrit comment l'information circule à l'intérieur de l'unité, de l'organisation et de la structure, est d'une importance clé pour la quatrième étape de l'ATG, qui consiste à déterminer les plans d'action de l'adversaire. De la même façon, une compréhension de la façon dont l'information en provenance de l'extérieur de l'unité, de l'organisation ou de la structure de l'adversaire circule doit également être élaborée pour l'usage du commandant, et inclut les environnements informationnels locaux, régionaux et globaux. Les équipes de COCIM qui oeuvrent dans le pays peuvent grandement aider au processus.

25. La quatrième étape de l'ATG consiste à combiner le modèle de prise de décisions et le modèle d'infrastructure pour en arriver au modèle de plan d'action en OI de l'adversaire. Les divers plans d'action à la disposition de l'adversaire sont alors élaborés et analysés de manière que nous puissions déterminer comment utiliser au mieux les OI pour influencer, soutenir ou exécuter la mission dans son ensemble.

SECTION 6
ÉVALUATION DES DOMMAGES AU COMBAT

26. L'évaluation des dommages au combat (EDC) confirme ou invalide les estimations de renseignement antérieures et met à jour l'ATG.

Le système de renseignement évalue de façon continue l'efficacité de l'ensemble des opérations de combat sur l'adversaire, y compris les OI. L'EDC permet aux commandants d'ajuster les efforts des OI pour en maximiser les effets. Un aspect important de l'EDC consiste à effectuer une analyse opportune visant à déterminer si un point vulnérable exploitable a été créé dans la structure de commandement et de contrôle de l'adversaire. Comparativement à la façon dont nous envisageons les procédures de production de rapports d'EDC classiques, l'EDC relative aux OI est plus difficile à effectuer.

27. L'EDC en matière d'OI ne se détermine pas toujours en termes de destruction matérielle d'objectifs. Le défi de l'EDC est de parvenir à évaluer les effets de nos efforts sans le bénéfice d'une confirmation matérielle. Les effets peuvent être des tendances, des activités ou des constantes dans les actions futures de l'adversaire. Ils peuvent consister en une simple absence d'activité dans un réseau de commandement et de contrôle donné, combinée à une augmentation de trafic ailleurs, c'est-à-dire des transmissions en ondes métriques/décimétriques (VHF/UHF) réduites couplées à une circulation accrue de courriers ou à une forte activité des lignes terrestres. L'EDC examine également le dommage collatéral que les actions de la guerre de commandement et de contrôle peuvent avoir causé à des systèmes non militaires et au potentiel au sein de l'EMI d'un commandant, par exemple l'effondrement des télécommunications commerciales, ou une augmentation significative des restrictions de sécurité ou de la propagande officielle dans les médias.

CHAPITRE 5
RENSEIGNEMENT, SURVEILLANCE, ACQUISITION D'OBJECTIF ET RECONNAISSANCE DANS LES OPÉRATIONS TERRESTRES

Et Moïse les envoya reconnaître la terre de Canaan; il leur dit de se diriger vers le sud et d'aller dans la montagne : voyez ce qu'est le pays; ce qu'est le peuple qui l'habite, fort ou faible, clairsemé ou nombreux.

Nombres 13:18-19

SECTION 1
INTRODUCTION

1. Le présent chapitre vise à expliquer le concept de renseignement, surveillance, acquisition d'objectif et reconnaissance (ISTAR), ainsi que son articulation avec le processus de sélection des objectifs au niveau de la formation et la capacité de perception de la situation. L'acronyme RISTA (reconnaissance, renseignement, surveillance et acquisition d'objectif) a été utilisé jusqu'à maintenant, mais est compris par certains comme indiquant que la reconnaissance est à la base du processus et en est le plus important composant. Le présent manuel a choisi d'utiliser l'acronyme ISTAR, de façon à mettre l'accent sur la prédominance du rôle de coordination du renseignement dans le processus sans cependant oublier que le seul but de l'ISTAR est d'appuyer le commandant dans son processus décisionnel. L'ISTAR n'est pas une fin en soi.

2. La plupart des visions des opérations futures reconnaissent que l'âge de l'information est, et continuera à être, caractérisé par la prolifération des systèmes d'information et la transmission rapide de l'information. La collecte, le contrôle et l'exploitation de cette information, par tous les moyens, sont des exigences préalables au succès des opérations militaires. Ceci vaut pour l'éventail complet des opérations possibles, des opérations autres que les combats aux opérations de combat. Le présent chapitre porte toutefois principalement sur les opérations de combat.

3. La doctrine militaire canadienne est de type manoeuvriste dans son approche en matière d'opérations. L'essence de l'approche manoeuvriste en matière d'opérations consiste à anéantir la cohésion de l'ennemi et à détruire sa volonté de combattre sans nécessairement s'engager dans une action à grande échelle. Pour y parvenir, il faut

déterminer les principaux points faibles de l'ennemi et les exploiter en concentrant la force ou en amenant l'ennemi à croire qu'une force décisive sera bientôt utilisée. Un potentiel du système ISTAR complet est essentiel au succès d'une approche manoeuvriste. Il permet aux commandants de travailler à l'aide du cycle de décision-action de l'ennemi et de livrer avec succès des batailles rapides et à actions multiples sans pertes inutiles pour les forces amies.

4. Les exigences propres à chaque opération dictent l'organisation et l'utilisation des ressources du système ISTAR. À chaque opération correspond un ensemble unique de besoins d'information, besoins dont la satisfaction est assurée par allocation de tâches à un large éventail de ressources du système ISTAR.

SECTION 2
LE CONCEPT DU SYSTÈME ISTAR

5. Le système ISTAR fait le lien entre la surveillance, l'acquisition d'objectif et la reconnaissance dans le but d'améliorer la capacité de perception de la situation d'un commandant, et de donner le signal aux ressources de manœuvre et d'assaut.

6. Le système ISTAR se définit comme une structure au sein de laquelle l'information recueillie par observation systématique est intégrée à l'information fournie par des missions spécifiques et traitée de manière à répondre aux besoins de renseignement du commandant. Ce système permet également de détecter, identifier et repérer des objectifs d'une façon suffisamment détaillée et opportune pour que les systèmes d'armes puissent engager le combat avec succès. Le système ISTAR se compose des éléments suivants :

a. des capteurs qui servent de ressources de collecte;

b. des processeurs qui servent de systèmes de collecte et d'analyse d'information;

c. un système de gestion de l'information et des capteurs;

d. un système efficace qui fait le lien entre les ressources du système ISTAR et le commandant.

7. La base du système ISTAR est que toutes les ressources d'ISTAR à un niveau donné de commandement sont contrôlées et gérées centralement par un coordonnateur ISTAR unique. Cette fonction est assurée par un Centre de recherche et d'analyse du renseignement (CRAR) ou, au niveau des unités, par le personnel du renseignement. Les

services de renseignement fournissent aux commandants et au personnel des renseignements opportuns et exacts sur l'ennemi, les conditions météorologiques et le terrain, ainsi que de l'information pertinente. Le concept d'ISTAR génère la synergie nécessaire en :

a. fournissant la combinaison de ressources de collecte et de technologies de système d'information requise à chaque niveau de commandement;

b. utilisant les technologies appropriées pour intégrer et coordonner le processus de collecte d'ISTAR;

c. améliorant le partage et la diffusion d'information/renseignement.

8. Le système ISTAR, lorsque bien conçu et mis en œuvre de façon appropriée, fournit la combinaison la plus appropriée de personnel, de matériel, et de procédures de commandement et de contrôle pour :

a. reconnaître des objectifs ou zones spécifiques;

b. maintenir une surveillance tout temps continue et systématique des airs, de la surface et du spectre électromagnétique dans une zone d'opérations;

c. transformer l'information recueillie en produits de renseignement de toutes sources.

9. Les besoins d'information, les ressources, le temps disponible et le risque déterminent la combinaison de ressources ISTAR utilisée.

SECTION 3
LES PRINCIPES DU SYSTÈME ISTAR

10. Les principes applicables en matière d'ISTAR peuvent se résumer comme suit :

a. **Coordination centralisée.** Les activités d'ISTAR doivent être coordonnées au plus haut niveau de commandement sans que le principe du commandement de mission soit sacrifié, ce qui assure l'utilisation la plus efficace et efficiente des ressources.

b. **Réponse.** Le système doit être en mesure de réagir rapidement aux besoins d'information et de renseignement du commandant, et d'exploiter rapidement l'information sur le choix des objectifs.

c. **Couverture continue.** La surveillance, l'acquisition d'objectif et la reconnaissance doivent être en mesure de fournir une couverture tout temps 24 heures sur 24, sept jours par semaine.

d. **Robustesse**. Les ressources du système ISTAR doivent fournir une combinaison robuste de systèmes se recoupant sur les plans de la technologie, de la portée et des performances, de manière à faire face à l'action de l'ennemi, ainsi qu'aux diverses conditions météorologiques et d'éclairement, et de déjouer les plans de déception de l'adversaire.

e. **Opportunité.** L'information et le renseignement doivent être fournis au commandant d'une manière opportune pour permettre à ce dernier de travailler dans le cadre du cycle de décision-action de l'ennemi.

f. **Exactitude**. Le produit ISTAR doit être précis et pertinent pour l'opération qu'il soutient.

g. **Transmission de l'information**. À l'intérieur d'un système ISTAR, il doit être possible de transmettre de l'information entre les commandants et états-majors appropriés sans que ceux-ci soient surchargés de données non pertinentes.

SECTION 4
LES ACTIVITÉS DU SYSTÈME ISTAR

11. Les définitions qui suivent sont essentielles à la compréhension dyu système ISTAR :

a. **Renseignement.** Résultat de l'exploitation des renseignements bruts concernant les nations étrangères, les forces armées ennemies ou pouvant le devenir, les zones où des opérations sont effectivement menées ou pourraient l'être (AAP-6(U) *Glossaire OTAN de termes et définitions*).

b. **Surveillance du champ de bataille**. Observation systématique de la zone de combat pour fournir en temps opportun le renseignement brut et le renseignement de combat (AAP-6 (U)).

c. **Acquisition d'objectif**. Opération consistant à détecter, localiser et identifier un objectif avec une précision suffisante pour permettre son traitement par une arme donnée (AAP-6(U)).

d. **Reconnaissance**. Mission entreprise en vue d'obtenir, par observation visuelle ou par d'autres modes de détection, des renseignements bruts sur les activités et les possibilités d'un ennemi actuel ou en puissance, ou d'acquérir des données concernant les caractéristiques météorologiques, hydrographiques ou géographiques d'une zone particulière (AAP-6(U)).

12. Les éléments du système ISTAR sont étroitement liés et se chevauchent souvent. Ils incluent les aspects ci-dessous :

a. **Surveillance de zone**. La surveillance continue d'une zone permet la collecte d'information générale sur un ennemi ou un ennemi possible. Elle peut servir à :

(1) fournir de l'information de base sur les déploiements, les niveaux d'activité, le potentiel et les intentions générales;

(2) donner des indices aux ressources de reconnaissance et d'acquisition d'objectif en vue de l'investigation d'activités spécifiques ou pour obtenir des données/information plus détaillées sur une observation en particulier;

(3) fournir une sécurité limitée aux forces amies grâce à une alerte avancée en cas d'activité ennemie à l'intérieur d'une trouée, sur des flancs exposés ou à l'arrière;

(4) aider à la reconnaissance et à l'identification avancées d'objectif.

b. **Reconnaissance en profondeur**. La reconnaissance en profondeur vise à fournir une information détaillée sur les secteurs au-delà de la portée des armes en tir à vue; elle peut être lancée à la suite d'une surveillance de zone ou de déductions des services de renseignement, et peut inclure :

(1) l'identification de forces ennemies connues ou suspectées, y compris leur composition et leurs activités,

(2) l'acquisition d'objectifs à l'intention des systèmes d'armes aériens, des systèmes d'armes en tir indirect et de l'aviation,

(3) le repérage et la poursuite d'unités, d'éléments ou d'activités de l'ennemi visés de façon spécifique.

c. **Reconnaissance rapprochée.** La reconnaissance rapprochée satisfait aux besoins tant d'information de combat et que d'acquisition d'objectifs essentiels aux troupes en contact ou quasi-contact avec l'ennemi.

d. **Acquisition d'objectif.** L'acquisition d'objectif est le processus qui consiste à fournir de l'information détaillée et à repérer les forces avec une exactitude suffisante pour permettre la sélection de ces éléments comme objectifs. Elle inclut :

(1) **l'acquisition d'objectif pour les armes en tir à vue** – normalement associée à une arme spécifique, un tel système fournit de l'information de combat essentielle sur un ennemi déjà repéré, et avec lequel le combat peut être engagé immédiatement;

(2) **l'acquisition d'objectif pour les armes en tir indirect** – normalement, un moyen de collecte de données/information oeuvrant au-delà de la ligne de vision des forces amies et fournissant de l'information à un système d'armes de tir indirect ou plus.

SECTION 5
SOURCES ET ORGANISMES

13. **Généralités**. La différence entre une source et un organisme est que la première fournit de l'information et le second, du renseignement. Différentes sources utilisent une variété de techniques et de disciplines pour acquérir leur information. Les composantes du renseignement, à savoir, le renseignement sur les transmissions (SIGINT), le renseignement humain (HUMINT), le renseignement par des techniques de

représentation (IMINT), le renseignement de source ouverte (OSINT) et le renseignement acoustique (ACOUSTINT), sont expliquées dans la B-GL-351-001/FP-001, *Renseignement de combat*. Les agences de renseignement requièrent normalement la contribution d'un certain nombre de sources, et quelquefois d'autres agences, avant de faire une évaluation.

14. **Sources.** Les sources incluent :

a. les troupes de jalonnement, de garde et de couverture;

b. les détachements de sûreté;

c. les unités, patrouilles et observateurs avancés;

d. la reconnaissance par des spécialistes et des troupes;

e. des avions, hélicoptères et véhicules aériens télépilotés (UAV);

f. les ressources de guerre électronique;

g. les prisonniers et réfugiés.

15. **Organismes.** Les organismes incluent :

a. l'état-major du renseignement (G2, artillerie, génie ou unité) du QG du groupement tactique, de la brigade, de la division et du corps d'armée,;

b. les états-majors du G3, du renseignement aérien et de GE du QG de la brigade, de la division et du corps d'armée;

c. l'organisation de patrouilles de reconnaissance lointaine;

d. la cellule de coordination SIGINT/GE du corps d'armée;

e. l'organisation d'interrogation.

16. Au niveau du corps d'armée, de la division et de la brigade, les organismes sont regroupés en un Centre de recherche et d'analyse du renseignement (CRAR) en vue de la coordination du traitement et de la collecte du renseignement.

SECTION 6
PLANIFICATION ET EXÉCUTION DU PROCESSUS D'ISTAR

17. **Planification.** Le processus menant au plan d'ISTAR se compose des étapes ci-dessous :

a. analyse de la mission;

b. établissement des besoins prioritaires en renseignement (BPR);

c. détermination des zones d'intérêt désignées et des zones d'intérêt comme objectif;

d. élaboration du plan de collecte.

18. **Exécution.** Un plan de collecte détaillé est essentiel à une utilisation efficace des ressources ISTAR de toute formation. Avant de procéder à toute assignation de tâche, le commandant et son état-major doivent :

a. analyser et valider la nécessité de tenir l'activité ISTAR considérée;

b. déterminer le degré de priorité du besoin;

c. passer en revue toutes les ressources ISTAR disponibles et sélectionner la plus appropriée;

d. demander aux formations supérieures et environnantes l'information et le renseignement requis sur les secteurs au-delà de leur zone d'opérations, en indiquant le degré de priorité applicable.

19. Après que la nécessité d'une tâche ISTAR ait été validée et approuvée, la tâche doit être attribuée à un système de collecte ou plus. En ce qui touche la collecte à l'extérieur de la zone de responsabilité de renseignement de la formation ou auprès d'organismes qui ne relèvent pas du commandement, une demande doit être présentée par l'entremise des quartiers généraux supérieurs. Les organismes peuvent inclure :

a. **Systèmes terrestres.** Passifs, actifs ou hybrides (passifs jusqu'à leur déclenchement).

b. **Systèmes aériens.** Passifs ou actifs.

c. **Systèmes satellite/spatiaux.**

d. **Systèmes d'information**.

20. Grâce aux progrès de la technologie, le traitement partiel rapide, les évaluations initiales et le traitement complet du renseignement sont devenues des parties intégrantes de toute activité ISTAR. Les capacités de traitement inhérentes de certaines ressources ISTAR sont telles que de l'information précieuse peut être dérivée du système pendant l'exécution même de la mission. On doit en conséquence prévoir des dispositions appropriées en vue de la diffusion opportune tant de l'information non traitée que de l'information obtenue grâce au combat, ainsi que du produit de renseignement traité final.

21. Une fois la tâche ISTAR terminée, les résultats obtenus doivent être évalués par rapport au besoin initialement défini dans le plan de collecte. On doit également décider si le besoin a été satisfait ou n'est plus valide. Le plan est alors mis à jour et une action additionnelle est lancée au besoin. Sans égard à ce qui précède, le cycle de renseignement est un processus dynamique et continu. Le besoin de renseignement et les priorités relatives changent constamment, et doivent être révisés régulièrement.

SECTION 7
LE PROCESSUS DE CHOIX DES OBJECTIFS

22. **Introduction**. Le choix des objectifs se définit comme étant « *le processus qui consiste à sélectionner des objectifs et à leur faire correspondre la réaction appropriée, en prenant en compte les besoins et le potentiel opérationnels* ». Il fusionne les ressources ISTAR et les systèmes d'armes, comme les systèmes aériens, l'aviation, les systèmes de tir indirect et les opérations de renseignement offensives, en garantissant que les capacités de chacun sont utilisées de manière à produire l'effet maximal. Un bon choix des objectifs est fondamental à la vitesse de réaction et est donc une responsabilité du G3 coordonnée dans le cadre du concept global des opérations. La contribution du G2 est toutefois manifestement importante.

23. **Niveau de commandement**. Un choix efficace des objectifs exige du temps, une contribution de l'état-major, et un accès à l'éventail complet des systèmes ISTAR et systèmes d'armes. Il est donc principalement mis en œuvre au niveau de la division ou à un niveau plus élevé, et optimisé en vue de l'engagement du combat contre des objectifs en profondeur. Les principes peuvent toutefois être appliqués au niveau de la brigade ou à un niveau moins élevé moyennant les modifications appropriées.

24. **Concept.** Le choix des objectifs fait partie intégrante du processus de planification, et exige un effort coordonné de plusieurs bureaux d'état-major. Il commence avec la réception de la mission, et est par la suite inextricablement lié au processus de planification opérationnelle (PPO) et à l'analyse tactique graphique (ATG) alors que le plan global est mis au point. Le cycle de choix des objectifs se compose de quatre phases comme suit.

a. **Décider.** Le plus grand nombre possible de décisions sont prises pendant le processus de planification, de manière que le choix des objectifs puisse être effectué dès que l'occasion s'en présente et sans qu'il soit nécessaire de consulter le commandant. Les priorités doivent être définies pour les aspects suivants :

(1) l'allocation des tâches aux ressources d'acquisition d'objectif;

(2) le traitement de l'information;

(3) l'utilisation des ressources d'assaut;

(4) le besoin d'une évaluation des dommages au combat (EDC).

b. **Détecter.** Si certaines ressources d'acquisition d'objectif peuvent fournir des objectifs réels, le produit d'information fourni par d'autres ressources doit être évalué pour permettre la détection d'objectifs. Une fois identifiés, les objectifs doivent être observés jusqu'à ce que le combat puisse être engagé. Les ressources utilisées à cette fin ne seront pas disponibles pour la détection de nouveaux objectifs.

c. **Exécuter.** Au cours de cette phase, les objectifs sont attaqués conformément aux priorités du commandant définies au cours de la phase de décision.

d. **Évaluer.** Les résultats d'une attaque doivent être évalués pour garantir que l'effet visé a été obtenu.

25. Le choix des objectifs facilite la coordination des ressources ISTAR et des ressources d'assaut, comme les systèmes aériens, l'aviation, les systèmes à tir indirect et les OI offensives, en garantissant qu'elles sont bien intégrées et que le système d'armes le plus approprié est utilisé pour l'attaque de chaque objectif. On trouvera de l'information

additionnelle sur ce sujet dans la B-GL-300-007/FP-001, *Puissance de feu de la Force terrestre*.

CHAPITRE 6
OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES

Le commandement est l'activité la plus importante d'une guerre. [4]

SECTION 1
INTRODUCTION

1. Le présent chapitre vise à expliquer les composantes offensives et défensives des Opérations d'information (OI). Les OI ne sont pas véritablement nouvelles. Ce qui est nouveau, c'est l'importance accrue accordée au commandement et à l'influence des convictions des personnes dans la zone d'opérations. Sans un commandement et un contrôle efficaces, la force militaire échouera même si elle possède la supériorité des armes et du nombre. La même chose est vraie de la cohésion des populations.

2. Un important sous-ensemble des OI offensives et défensives a pris le nom de guerre de commandement et de contrôle. À l'époque où la guerre de commandement et de contrôle visait principalement les systèmes de commandement et de contrôle, elle était trop restrictive par rapport à l'application réelle des OI au cours des opérations. La définition des OI offensives et défensives a donc été élargie de manière à englober l'influence des convictions des populations dans la zone d'opérations, ainsi que les activités de contre-ingérence (CI), les opérations contre-psychologiques (contre-PSYOPS), l'attaque des réseaux d'ordinateurs (ARO) et les OI spéciales (OIS).

3. Les OI offensives et défensives ne sont rien de plus qu'une approche coordonnée consistant à attaquer la capacité d'un adversaire à commander, y compris l'influence des convictions des populations hostiles et neutres, tout en garantissant que notre commandement demeure efficace et que notre population est protégée. En tant que parties intégrantes des OI, les OI offensives et défensives appuient l'approche manoeuvriste de l'Armée de terre en matière d'opérations.

4. Les méthodes et moyens dont nous disposons pour attaquer les systèmes de commandement et de contrôle d'un pays adversaire ont

---

[4] B-GL-300-003/FP-000, *Commandement*

augmenté de manière importante. Il en résulte une augmentation parallèle des points vulnérables. Pour être efficaces, les OI doivent être pleinement intégrées au concept des opérations du commandant et être coordonnées avec ces dernières.

5. La guerre de commandement et de contrôle se définit comme étant « *l'utilisation intégrée de la totalité des capacités militaires, y compris la sécurité des opérations (OPSEC), la déception, les opérations psychologiques (OPSPSY), la guerre électronique (GE) et la destruction matérielle, soutenues par l'ensemble des systèmes de renseignement et de communications (SIC) de base, dans le but d'empêcher l'accès à l'information de l'infrastructure de commandement et de contrôle d'un adversaire, ainsi que d'influencer, de dégrader ou de détruire cette infrastructure, tout en protégeant l'infrastructure de commandement et de contrôle amie contre des actions similaires* »[5].

6. Les OI offensives et défensives soutiennent directement le but qui consiste à parvenir à la supériorité de l'information et à gagner tout conflit, y compris les opérations autres que la guerre, rapidement, de façon décisive et avec un minimum de pertes. Cette combinaison d'aspects offensifs et défensifs en une capacité intégrée fournit des possibilités accrues de synergie au cours d'une guerre. Les OI permettent à l'Armée de terre et aux commandants individuels de s'acquitter des missions avec moins de risques, dans des délais plus courts et avec moins de ressources.

RÔLE DES OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES

7. Les OI offensives et défensives peuvent être appliquées à toutes les phases d'une opération, y compris avant, pendant et après les hostilités. Même pendant les opérations autres que la guerre, elles procurent au commandant militaire des moyens létaux et non létaux de s'acquitter de la mission assignée tout en dissuadant de faire la guerre et/ou en favorisant la paix. L'aspect offensif des OI peut ralentir le rythme opérationnel de l'adversaire, perturber ses plans et sa capacité à concentrer la puissance de combat, et influencer son estimation de la situation. L'aspect défensif des OI minimise les points de vulnérabilité du personnel et du système de commandement et de contrôle amis, ainsi que l'interférence mutuelle de ces points. Les OI offensives et défensives

---

[5] MC 348 *Politique de commandement et de contrôle en situation de guerre de l'OTAN*

s'appliquent à l'ensemble des situations de conflit. Les OI défensives ne seront normalement pas restreintes au temps de paix, mais les OI offensives feront l'objet d'un contrôle par l'entremise des Règles d'engagement (RE).

SECTION 2
ÉLÉMENTS

8. Un SIC robuste, ainsi que le soutien continu aux niveaux national/tactique que procurent l'information pertinente et le renseignement, sont le fondement des OI. Les éléments des OI offensives et défensives sont les suivants :

a. OPSEC;

b. la contre-ingérence (CI);

c. la déception militaire;

d. OPSPSY

e. contre-OPSPSY;

f. la guerre électronique (GE);

g. ARO;

h. OIS;

i. la destruction matérielle.

9. Ces éléments contribuent à la protection de la force et à l'exécution de la mission de différentes façons, selon la situation. L'utilisation intégrée de ces éléments mène à une synergie sur le champ de bataille et résulte dans l'exécution la plus efficace possible des OI offensives et/ou défensives en concentrant les attaques sur l'adversaire, son commandant et la capacité de ce dernier à commander et contrôler les forces ennemies, tout en protégeant les forces et l'infrastructure de commandement et de contrôle amies.

INFORMATION PERTINENTE

10. Le succès des OI offensives et défensives au cours des opérations dépend de façon critique d'une information et d'un renseignement exacts, pertinents et opportuns. Pour assurer le succès des OI offensives, il est nécessaire de déterminer qui sont les commandants de l'adversaire et leurs systèmes de soutien. De plus, les commandants d'aujourd'hui doivent comprendre quels sont les points vulnérables de nos propres systèmes et

prendre les mesures nécessaires pour nous protéger des attaques. Le nombre accru de ressources de renseignement, surveillance, acquisition d'objectif et reconnaissance (ISTAR) à la disposition d'un commandant, ainsi que la coordination des activités et produits s'y rapportant, ne peuvent plus être cloisonnés comme dans le passé.

SYSTÈMES D'INFORMATION ET DE COMMUNICATIONS

11. Les SIC sont d'une importance critique. Ce sont les pipelines qui permettent l'exécution des activités d'information (acquérir, empêcher, utiliser et protéger). Les SIC sont en conséquence un objectif majeur de notre effort d'OI offensives. La confiance que l'Armée de terre place dans son SIC maintenant et dans le futur a créé des points vulnérables importants pour les commandants et les systèmes de soutien du commandement. La connaissance de nos propres points vulnérables est la clé de la protection.

SÉCURITÉ DES OPÉRATIONS

12. La sécurité des opérations se définit comme étant « *l'ensemble des mesures qui donnent à une opération ou à un exercice militaires la sécurité adéquate par des moyens actifs ou passifs, afin d'interdire à l'ennemi la connaissance du dispositif, des moyens et des intentions des forces amies.* »[6]

13. Les activités d'OPSEC donne au commandant la possibilité d'identifier les actions qui peuvent être observées par les systèmes de renseignement de l'adversaire. Elles sensibilisent aux indicateurs amis que les systèmes de renseignement adverses peuvent obtenir. Cette connaissance peut être interprétée ou réunie de manière à dériver de l'information critique sur les dispositions, l'intention, et/ou les plans d'action de la force amie qui doivent être protégés. Le but des activités d'OPSEC est de déterminer, sélectionner et exécuter les mesures qui éliminent ou réduisent à un niveau acceptable les indications et autres sources d'information qui pourraient être exploitées par un adversaire.

14. La planification des activités d'OPSEC fait face aux défis multiples posés par la nouvelle famille des capacités commerciales globales, dont les systèmes d'imagerie, les systèmes de positionnement et

---

[6] NATO AAP 6 (U)

les systèmes cellulaires, qui offrent à des adversaires possibles l'accès à un niveau sans précédent d'information contre les forces amies. La présence inévitable des médias d'information pendant les opérations militaires complique l'OPSEC. La capacité des médias à transmettre de l'information en temps réel à un auditoire mondial pourrait être une source lucrative d'information pour un adversaire. Les planificateurs des activités d'OPSEC doivent, en collaboration étroite avec le personnel des Affaires publiques (AP), élaborer les éléments essentiels d'information sur les forces amis (EEIFA) qui serviront à prévenir la divulgation par inadvertance d'information critique ou sensible.

15. De nombreuses mesures ont une incidence sur l'OPSEC. Ces mesures incluent la CI, la sécurité de l'information (INFOSEC), la sécurité des émissions (TRANSEC), la sécurité des communications (COMSEC) et la sécurité des transmissions (SIGSEC). L'importance de l'INFOSEC grandit à mesure que la force se numérise.

CONTRE-INGÉRENCE

16. La CI se compose des activités de renseignement liées à l'évaluation des points vulnérables aux capacités de renseignement d'un adversaire, comme un système ISTAR, et à la neutralisation de ces points vulnérables. La CI agit en réponse à la fois au renseignement de sécurité (SECINT) et au renseignement de combat, et soutient l'OPSEC. Se reporter à la B-GL-352-001/FP 001, *Renseignement de combat* pour une étude détaillée de la question.

DÉCEPTION MILITAIRE

17. La déception se définit comme étant « *les mesures visant à induire l'ennemi en erreur, grâce à des truquages, des déformations de la réalité, ou des falsifications, en vue de l'inciter à réagir d'une manière préjudiciable à ses propres intérêts* »[7]. La déception militaire est le principal moyen d'influence des décisions du commandant adversaire par l'entremise de la distortion, de la dissimulation et/ou de la falsification des intentions, de l'état, des dispositions, des capacités, des plans d'action et des points forts des forces amies. Le but de la déception est d'amener le commandant militaire adverse à agir d'une manière utile aux objectifs du commandant ami.

---

[7] NATO AAP 6 (U)

PERSPECTIVE HISTORIQUE

La déception tactique a eu des répercussions positives importantes sur le succès de l'opération OVERLORD et, ainsi, sur la reprise du continent européen au cours de la Deuxième Guerre mondiale. La déception a collaboré étroitement avec les OPSEC pour cacher soigneusement l'organisation et l'emplacement des véritables cantonnements, lieux d'entraînement, dépôts temporaires, mouvements et embarcations. Des efforts incroyables ont été consacrés à la création de faux terrains d'aviation et ports, navires, bateaux, avions, chars d'assaut, véhicules et mouvements de troupe, tant réels que feints. Une nouvelle ère de déception commençait – l'ère de la déception électronique. Les radars de la défense côtière allemande ont été détruits selon un modèle déterminé. Les planificateurs des opérations de déception avaient intentionnellement laissé intacts un certain nombre de radars dans la région de Calais. La nuit où l'invasion a été lancée, les Alliés ont commencé à brouiller massivement les radars allemands au moyen de paillettes. Mais sans couvrir entièrement leurs objectifs. Les opérateurs de radar allemands pouvaient « voir » entre les rideaux de brouillage des Alliés. Et ce qu'ils ont vu, c'était une flotte fantôme de petits navires remorquant des barges et des dirigeables, et se dirigeant vers Calais à une vitesse de huit nœuds – ce qui est la vitesse d'une flotte amphibie. Des émetteurs électroniques puissants recevaient l'impulsion des radars allemands et la renvoyaient avec force à ces derniers. À chaque répétition de cette déception, les opérateurs allemands croyaient détecter la présence d'un navire de 20 000 tonnes. Les petits navires étaient également équipés de haut-parleurs et faisaient entendre des bandes sonores de l'assaut amphibie à Salerne à partir d'une distance de dix milles en mer. Les troupes allemandes à terre pouvaient entendre les Alliés « prendre place à bord de leurs péniches de débarquement » pour atteindre la plage. Cette information a semé le chaos chez le renseignement allemand pendant plusieurs heures précieuses, et a contribué de façon importante à retarder la riposte des Allemands à l'invasion réelle, qui se déroulait en Normandie.

OPÉRATIONS PSYCHOLOGIQUES

18. Les Opérations psychologiques se définissent comme étant « *des activités psychologiques planifiées, s'adressant en temps de paix comme en temps de guerre à des publics hostiles, amis ou neutres, et visant à influencer des attitudes et des comportements affectant la réalisation d'objectifs politiques et militaires* »[8].

---

[8] OTAN AJP 1

19. Les OPSPSY visent à pour transmettre de l'information et des indicateurs choisis à des auditoires étrangers dans le but d'influencer leurs émotions, leurs motifs, leur raisonnement objectif et, en bout de ligne, le comportement des gouvernements, organisations, groupes et individus étrangers. Le but des OPSPSY est d'induire ou de renforcer les attitudes et le comportement à l'étranger qui sont favorables aux objectifs de l'émetteur.

20. Les OPSPSY sont fondées sur la projection de la vérité et de messages crédibles. Les OPSPSY sont un outil essentiel dans les OI tant offensives que défensives. Les éléments des OPSPSY doivent être coordonnés avec les autres éléments de la guerre de commandement et de contrôle, ainsi qu'avec les stratégies d'AP, de manière à maximiser l'avantage des OI. Citons à titre d'exemple la force considérable montrée par l'Armée de terre dans l'application des OPSPSY aux opérations militaires à Haïti.

21. L'objectif principal des OPSPSY en matière d'OI défensives est de minimiser les effets de la campagne de propagande et de désinformation d'un adversaire à l'encontre des Forces canadiennes. Discréditer la propagande ou la désinformation contre les opérations des forces de coalition est critique au maintien d'une opinion publique favorable.

CONTRE-OPSPSY

22. Le but des contre-OPSPSY est de protéger un auditoire contre les messages hostiles et d'amoindrir l'impact de ces derniers. Dans ce contexte, les OPSPSY visent à contrer l'information, les convictions, les attitudes et le comportement nuisibles aux objectifs d'une opération des Forces canadiennes. Toute mauvaise information ou désinformation propagée sera exploitée par les extrémistes politiques, les groupes paramilitaires et militaires pour rallier le soutien de la population à leurs objectifs.

GUERRE ÉLECTRONIQUE

23. La guerre électronique se définit comme étant « *une action militaire consistant à utiliser l'énergie électromagnétique (EM), y compris l'énergie directe, pour exploiter et dominer le spectre EM ou attaquer un ennemi. Elle inclut l'interception et l'identification des émissions EM, l'utilisation d'énergie EM pour réduire ou prévenir une utilisation hostile du spectre EM et des actions visant à assurer l'usage*

efficace de ce dernier par les forces amies. Les trois divisions de la GE sont : les contremesures électroniques (CME), les mesures de protection électroniques (MPE) et les mesures de soutien de guerre électronique (MSGE) »[9].

24. Les CME sont le volet attaque de la GE. Les CME se définissent comme étant « *la partie de la GE qui a trait aux actions prises, au moyen d'énergie EM, pour interdire ou réduire l'utilisation efficace par l'ennemi du spectre EM* ». On distingue trois catégories de CME : le brouillage électronique, la déception électronique et la neutralisation électronique.[10] Les CME peuvent attaquer l'adversaire en tout point, à partir de ses formations tactiques jusqu'à son infrastructure nationale. (L'Armée américaine utilise l'expression « *attaque électronique* » (AE)).

25. Les MPE visent à protéger l'usage du spectre EM par les forces amies. Les MPE se définissent comme étant « *la partie de la GE qui a trait aux actions prises pour assurer une utilisation amie efficace de l'EM en dépit de l'usage d'énergie EM par l'ennemi* »[11]. Les MPE couvrent la totalité du personnel, du matériel et des installations. Les MPE font partie de la surviabilité. Ainsi, les systèmes d'autoprotection et de protection de la zone peuvent faire obstacle aux systèmes d'acquisition d'objectif et d'engagement de l'ennemi pour prévenir la destruction de forces et de systèmes amis. (L'Armée de terre américaine utilise l'expression « protection électronique » (PE)).

26. Les MSGF se définissent comme étant « *la partie de la GE qui a trait aux actions prises pour chercher, intercepter et identifier les émissions EM, et en repérer la source, dans un but de reconnaissance des menaces immédiates. Elle fournit une source d'information nécessaire en vue des décisions immédiates touchant les CME, MPE et autres actions tactiques* »[12].

27. L'information sur le conflit fournie par les MSGE inclut les actions assignées par un commandant ou sous le contrôle direct de ce

---

[9] ATP 51(A) *OTAN Guerre électronique dans la bataille terrestre*

[10] ATP 51(A)

[11] ATP 51(A)

[12] ATP 51(A)

dernier dans le but de chercher, intercepter, identifier et repérer les sources d'énergie EM intentionnelles et accidentelles, et de détecter les risques immédiats. Les MSGE sont l'essence même de l'information de combat et capitalisent sur l'opportunité des systèmes capteur-tireur. La meilleure description qu'on puisse faire des MSGE consiste à les assimiler à des opérations de reconnaissance et surveillance électroniques. Elles peuvent être conduites par des détachements individuels en soutien à des unités ou sous-unités, ou par des systèmes complets en soutien de formations.

28. La GE n'est plus seulement une question de spécialistes pour les unités spécialisées. La GE du futur visera de plus en plus la protection des objectifs de grande valeur, de la même manière que la Marine et la Force aérienne protègent les navires et les avions. La GE est un outil ISTAR important qui peut être utilisé seul, mais qui est considérablement plus efficace lorsqu'elle est utilisée en conjonction avec d'autres éléments ISTAR, comme les véhicules aériens télépilotés, comme parite intégrante d'un système coordonné.

ATTAQUE DES RÉSEAUX D'ORDINATEURS

29. L'attaque des réseaux d'ordinateurs se définit comme étant « l'ensemble des opérations visant à perturber, dégrader ou détruire l'information présente dans les systèmes d'information, ou ces systèmes d'information eux-mêmes »[13]. L'attaque des réseaux d'ordinateurs et les CME sont toutes deux des éléments des OI offensives, et les CME pourraient être utilisées dans le cadre d'une attaque des réseaux d'ordinateurs.

OPÉRATIONS D'INFORMATION SPÉCIALES

30. Les Opérations d'information spéciales se définissent comme étant « des OI particulières qui, en raison de leur effet possible, des exigences de sécurité ou du risque pour la sécurité nationale du Canada, requièrent un examen et un processus d'approbation spéciaux »[14].

---

[13] Ligne de conduite sur les opérations d'information des Forces canadiennes, 4e version préliminaire

[14] B-GG-005-004/AF-032, *Doctrine des opérations d'information des Forces canadiennes*

DESTRUCTION MATÉRIELLE

31. La destruction matérielle se définit comme étant « l'application de la puissance de combat pour détruire ou neutraliser les forces et installations ennemies. Elle inclut le tir direct et indirect des forces terrestres, navales et aériennes, ainsi que les actions directes des forces d'intervention spéciale ».

32. La destruction d'un objectif de commandement et de contrôle hostile signifie que le potentiel de commandement et de contrôle de l'adversaire est dégradé pour un certain temps ou anéanti de façon permanente. La destruction matérielle est utilisée seulement après une évaluation complète, des points de vue stratégiques et tactiques, des avantages comparatifs de la préservation de l'objectif et de sa destruction.

PERSPECTIVE HISTORIQUE

Le 14 avril 1943, les spécialistes américains du renseignement interceptaient et décodaient un message à l'effet que l'amiral Isoroku Yamamoto, commandant en chef de la Marine japonaise, allait se rendre à Bougainville en avion dans quatre jours. Lorsque l'analyse démontra que Bougainville se situait à l'intérieur du rayon d'action étendu des chasseurs US P-38 stationnés à Henderson Field, sur l'île de Guadalcanal, les planificateurs alliés virent là l'occasion de frapper au cœur du système de commandement et de contrôle et de la planification stratégique du Japon dans le Pacifique. En moins de 48 heures, les forces de l'amiral Chester W. Nimitz planifièrent et coordonnèrent une opération visant à abattre l'avion de Yamamoto, et obtinrent l'approbation du secrétaire à la Marine Frank Knox et du président Roosevelt.

La ponctualité de Yamamoto était proverbiale, et les planificateurs américains étaient confiants que son avion paraîtrait au-dessus de Bougainville à l'heure dite, soit 9 h 39, le 18 avril. Au moment convenu, seize chasseurs P-38 de la base de Henderson Field soigneusement positionnés aperçurent les deux bombardiers Betty japonais transportant Yamamoto et ses aides, et attaquèrent. Les deux avions furent rapidement envoyés au sol, ce qui mit fin à une opération d'information classique qui avait duré moins de quatre jours au total, et avait infligé des dommages irréparables au système de commandement et de contrôle japonais. Le Japon allait se ressentir des répercussions de cette unique mission jusqu'à la fin de la guerre.

SECTION 3
OPÉRATIONS D'INFORMATION OFFENSIVES

33. **OI offensives.** Les OI offensives se définissent comme étant « *l'exécution synchronisée des actions entreprises pour atteindre des objectifs établis dans le but de prévenir un commandement et un contrôle efficaces des forces adverses en empêchant l'accès à l'information de ces dernières, et en influençant, dégradant et détruisant l'infrastructure de commandement et de contrôle de l'adversaire, ou en influençant les convictions de personnes hostiles* ».

34. **Principes de base des OI offensives.** Les trois principes de base des OI offensives consistent à :

a. Planifier sur la base de la mission de l'unité, de l'intention du commandant et du concept des opérations.

b. Synchroniser le déroulement avec le plan du commandant et soutenir ce plan.

c. Prendre et conserver l'initiative en dégradant le SIC de l'adversaire et en forçant ce dernier à adopter une attitude réactive, c.-à-d. que les OI offensives ralentissent le rythme de l'adversaire, perturbent ses cycles de planification et de décision, perturbent la capacité de son commandant à mettre sur pied la puissance de combat, et dégradent les moyens à sa disposition pour exécuter les ordres de mission et contrôler les opérations des unités subordonnées.

35. **Effets des OI offensives.** D'une manière générale, les OI offensives ont quatre effets, lesquels sont axés sur l'infrastructure de commandement et de contrôle de l'adversaire, ainsi que sur son flux d'information, et visent à produire un cycle de prise de décisions de moindre qualité et plus lent. Ces effets sont les suivants :

a. En premier lieu, les OI offensives empêchent l'adversaire d'avoir accès à l'information en perturbant son observation, en dégradant son orientation et la formulation de ses décisions, et en dégradant sa collecte d'information. Il est possible de dégrader la collecte d'information en détruisant les moyens de collecte, en influençant l'information que l'adversaire acquiert ou en faisant en sorte que ce dernier ne puisse recueillir aucune information.

b. En deuxième lieu, les OI offensives influencent le commandant de l'adversaire en manipulant sa perception et en désorientant son cycle de décision.

c. Troisièmement, les OI offensives dégradent les OI de l'adversaire en perturbant sélectivement les systèmes de commandement, de contrôle, de communications, d'ordinateurs et de renseignement.

d. Quatrièmement, les OI offensives peuvent neutraliser les capacités d'information de l'adversaire ou les détruire par le truchement de la destruction matérielle

des nœuds et liens. Les opérations de destruction sont d'une efficacité maximale lorsqu'elles sont planifiées de manière à survenir juste avant que l'adversaire ait besoin d'une certaine fonction de commandement et de contrôle, ou visent un objectif qui fait appel à beaucoup de ressources et est difficile à reconstituer.

36. Les OI offensives peuvent également avoir une incidence importante sur les convictions et la cohésion des troupes et de la population ennemies. L'interaction de l'ensemble des éléments des OI offensives et défensives est étudiée en détail à l'annexe A.

PERSPECTIVE HISTORIQUE

Héraclite d'Éphèse, qui vécut au sixième siècle avant Jésus-Christ, avait fait remarquer que « si vous ne vous attendez pas à l'inattendu, vous ne le rencontrerez pas ». Lorsque les Allemands ont envahi l'Union soviétique, en juin 1941, ils ont repéré dans le système de commandement et de contrôle soviétique un certain nombre de défaillances exploitables que les Russes eux-mêmes n'avaient pas décelées. Utilisant les outils de la guerre de commandement et de contrôle de façon coordonnée, les Allemands ont réussi à perturber, exploiter et détruire le système de commandement et de contrôle soviétique. Au moyen d'armes spécifiquement construites pour la guerre de commandement et de contrôle, ils ont attaqué des éléments du système soviétique par la voie des airs, et au moyen de l'artillerie et de sabotage. Les résultats de ces attaques ont été surprenants. En raison des efforts de sabotage transfrontaliers des Allemands, de nombreuses unités soviétiques « n'ont pas reçu l'ordre d'état d'alerte lorsqu'il a été émis [de Moscou] dans la nuit du 20 au 21 juin 1941 ». Le 24 juin, des brèches importantes avaient déjà été pratiquées dans le réseau de communications des Soviétiques, forçant ainsi les commandants à utiliser des réseaux radio non protégés et facilement exploitables. Cette situation permit à son tour aux Allemands d'attaquer des postes de commandement exposés et leurs unités associées à la grandeur du théâtre. Ces attaques, en raison de leur efficacité, menèrent les commandants soviétiques à interdire l'utilisation des postes radios parce qu'ils pouvaient révéler les positions des forces amies. Au moyen de la guerre de commandement et de contrôle, les Allemands avaient réussi à neutraliser le système de commandement et de contrôle soviétique, créant un environnement opérationnel qui mena rapidement à un effondrement de l'ensemble du front est.

SECTION 4
OPÉRATIONS D'INFORMATION DÉFENSIVES

37. **OI défensives.** Les OI défensives se définissent comme étant *« le maintien du système de commandement et de contrôle de ses propres forces en tournant à l'avantage des forces amies ou en neutralisant les efforts de l'adversaire pour empêcher l'accès à l'information, influencer, dégrader ou détruire le système de commandement et de contrôle ami, de même que la protection de ses propres troupes, et du personnel ami et neutre, contre les effets des OI offensives de l'ennemi ».*

38. Les OI défensives peuvent être proactives ou réactives. Les OI défensives proactives utilisent les éléments des OI offensives et des OI défensives pour réduire la capacité de l'adversaire de mener des OI offensives. Les OI défensives réactives réduisent les points vulnérables aux OI offensives de l'ennemi au moyen d'une protection appropriée sur le plan du matériel, de l'électronique et du renseignement.

39. **Principes de base des OI défensives.** La meilleure façon de comprendre le processus des OI défensives consiste à faire une analyse inverse du processus d'OI offensives. Les commandants s'efforcent de déterminer comment l'adversaire peut utiliser la destruction, la guerre électronique, l'attaque des réseaux d'ordinateurs, la déception militaire, les OPSEC, les OIS et les OPSPSY pour perturber les systèmes de commandement et de contrôle amis, le processus de prise de décisions amis et les convictions de la population du Canada. Ayant simulé les plans d'action des OI offensives de l'adversaire, le commandant peut élaborer une position d'ensemble, en matière d'OI défensives, qui soit synchronisée avec l'effort principal et les OI offensives. Le commandant se guide sur les six principes de base des OI défensives. Ces principes sont les suivants :

a. Parvenir à la supériorité du commandement et du contrôle. Ce principe inclut des fonctions comme le traitement sans entrave de l'information, l'élaboration de plans d'action appropriés, une prise de décisions valide et des communications efficaces avec les subordonnés.

b. Avoir un cycle de décision plus rapide que celui de l'adversaire. Pour y parvenir, empêcher l'utilisation du personnel, du matériel, et des systèmes de commandement et de contrôle de l'adversaire, et les influencer, les dégrader et/ou les détruire.

c. Réduire la capacité de l'adversaire à mener des OI offensives.

d. Réduire les points vulnérables des systèmes de commandement et de contrôle amis au moyen de mesures d'OI défensives. Par exemple, contrer les effets de la propagande ou de la désinformation de l'adversaire en ayant recours aux OPSPSY et aux AP.

e. Réduire les interférences amies avec nos systèmes de commandement et de contrôle sur tout le spectre EM (éliminer les conflits et coordonner).

f. Garantir que les troupes et la population sont bien informés de la situation dans les limites des OPSEC.

PERSPECTIVE HISTORIQUE

L'histoire de l'Âge de l'information s'écrit maintenant. En 1988, nous avons été témoins du premier cas bien publicisé de virus informatique. Ce virus insidieux et autoreproducteur appelé le vers de l'Internet a pénétré dans le réseau informatique de l'Université de la Californie à Berkeley, corrompant des milliers d'ordinateurs reliés à Internet. L'équipe d'intervention d'urgence informatique créée à l'université Carnegie Mellon a décelé son premier cas important en 1993, avertissant alors les administrateurs du réseau qu'une bande d'intrus avait volé des dizaines de milliers de mots de passe Internet.

Lorsque l'équipe a été mise sur pied, à la fin des années 1980, elle traitait moins de 50 événements par année. Maintenant, elle traite des milliers de cas par année. L'armée est une des cibles de ces attaques. On a récemment signalé le cas d'un adolescent de seize ans qui avait compromis la sécurité de plus de 30 systèmes militaires et de plus de 100 autres systèmes, avant d'être attrapé au bout d'une chasse électronique internationale qui a duré 26 jours. Cette expérience donne un indice des incidences qu'un effort professionnel et bien financé pourrait avoir sur les réseaux d'ordinateurs.

La leçon que nous enseignent de façon saisissante ces événements est que l'autoroute de l'information accroît la vulnérabilité des Forces canadiennes. Nous sommes tous familiers avec la façon d'assurer la sécurité en ce qui touche la transmission de l'information par radio ou téléphone. Mais les ordinateurs, les bases de données, les logiciels (comme les aides et les outils de prise de décisions), les serveurs, les routeurs et les commutateurs créent une vulnérabilité encore plus grande, laquelle existe aujourd'hui et progresse géométriquement.

40. **Effets des OI défensives.** Les effets des OI défensives sont l'inverse des effets des OI offensives. Nous pouvons empêcher l'adversaire d'avoir accès à l'information dont il a besoin pour prendre des mesures efficaces. Nous pouvons influencer l'adversaire de manière qu'il ne pose pas de geste, qu'il pose le mauvais geste ou qu'il pose un geste au mauvais moment. Nous pouvons dégrader et détruire ses capacités d'OI offensives contre les forces amies. Les contre- OPSPSY et les AP soutiennent les OI défensives. Les OPSPSY peuvent creuser un écart entre le leadership de l'adversaire et sa population, de manière à miner la confiance et l'efficacité du leadership de l'adversaire. Le

programme d'information interne du commandant, diffusé par l'officier des Affaires publiques (OAP), peut être extrêmement bénéfique en contrant la propagande de l'adversaire au Canada et au sein de forces déployées. Les spécialistes des AP, en collaboration avec le personnel des OPSPSY et du renseignement, peuvent également élaborer des produits d'information que les commandants peuvent utiliser pour aider à protéger les soldats contre les effets des efforts de mauvaise information ou de désinformation de l'adversaire.

SECTION 5
COORDINATION

41. La publication B-GL-300-003/FP-000, *Commandement*, examine l'importance du commandement. Les OI sont une fonction de commandement qui vise directement l'adversaire et son commandant tout en nous protégeant. Si tous les commandants ne disposent pas nécessairement de toutes les capacités au sein de leur unité pour agir dans tous les domaines des OI offensives et défensives, il est impératif qu'ils reconnaissent tous quelles activités ils peuvent mener et comprennent leur portion d'un plan plus large.

42. Il incombe au G3/CEM de planifier et coordonner les OI au nom du commandant. IL NE S'AGIT PAS UNE ACTIVITÉ DE SPÉCIALISTE. Au niveau de la formation, un officier des OI peut être désigné pour aider le G3/CEM à planifier et coordonner l'effort d'OI de la formation. Des conseillers spécialisés seront nécessaires en fonction des capacités d'OI de la formation. Une annexe OI devrait accompagner tous les ordres d'opérations. Les activités de coordination et de planification des OI doivent être menées en conformité avec les dispositions contenues dans la B-GL-331-001/FP-001, *Doctrine de soutien du commandement*.

CHAPITRE 7
AFFAIRES PUBLIQUES

Une presse hostile est davantage à craindre que cinq corps d'armée.

Napoléon

SECTION 1
INTRODUCTION

1. Le champ de bataille moderne a changé de façon phénoménale et la capacité des médias à faire rapport sur la situation à partir du champ de bataille a elle aussi beaucoup changé. Les progrès technologiques font en sorte que les opérations futures se dérouleront devant un auditoire mondial. Les mesures tactiques et les difficultés des soldats et des civils auront une incidence croissante sur la prise de décisions stratégique.Les images en temps réel des opérations, tant positives que négatives, continueront d'influencer la compréhension et le soutien du public. Par exemple, en 1992, les soldats américains ont débarqué sur les plages de Mogadishu sous l'éclairage des projecteurs de caméras de télévision, et les images ont été diffusées en direct partout dans le monde. En 1996, les soldats canadiens arrivant à l'aéroport de Kigali, au Rwanda, pour l'opération Assurance ont été accueillis par un barrage médiatique similaire et leurs actions ont été télédiffusées à un auditoire européen presque en direct.

2. La présence des médias d'information est essentiellement devenue une réalité du champ de bataille. Cette réalité doit être prise en considération dans la planification des opérations militaires. Les capacités et besoins des médias d'information doivent être compris et considérés par les planificateurs. Un échec à cet égard n'empêchera pas les médias de couvrir les opérations car ils iront à d'autres sources pour leur information et créeront peut-être ce faisant une situation qui compromettra le succès de l'opération qu'ils essaient de couvrir.

3. Les commandants, qui possèdent l'information et la capacité requises pour donner forme à toutes les dimensions de la zone d'opérations, peuvent organiser et contrôler les forces avec la rapidité et le synchronisme nécessaires pour gagner. Les besoins d'information du commandant ne sont pas satisfaits par une source unique, mais par une combinaison de nombreux systèmes et fonctions, dont les médias d'information.

SECTION 2
ENVIRONNEMENT DE L'INFORMATION

4. L'environnement global de l'information (EGI) contient les processus et systèmes d'information qui sont hors de l'influence militaire directe, mais qui peuvent avoir une incidence directe sur le succès ou l'échec des opérations militaires. Les médias, les organisations internationales et même les individus font partie de l'EGI.

5. Toutes les opérations de l'Armée de terre peuvent être influencées par les messages planifiés ou non communiqués par l'entremise de l'EGI. Les nouvelles des opérations militaires peuvent être diffusées en temps réel ou presque réel à nos troupes, au public canadien, à nos alliés, à nos adversaires, en fait, à toute force belligérante impliquée dans une opération. L'analyse publique, les critiques et les commentaires officieux peuvent avoir des répercussions sur les opérations en cours. Des débats peuvent commencer (et être gagnés ou perdus) avant que les chefs militaires aient eu le temps d'évaluer les problèmes et de mettre au point un plan de réponse. De tels débats peuvent influer sur les buts stratégiques, la processus de décision, les opérations tactiques, le moral et l'efficacité générale de la force en cause. Dans les faits, l'EGI étend la zone d'opérations à toute la planète, et est une source d'information si importante qu'il doit être pris en considération dans tous les efforts de planification opérationnelle.

6. L'environnement militaire de l'information (EMI) se compose des systèmes d'information et organisations, tant amis qu'ennemis (ou appartenant à une des factions belligérantes dans les opérations autres que que la guerre), militaires et non militaires qui soutiennent, favorisent ou influencent de façon significative les opérations militaires. La réussite d'une mission est fonction de la supériorité de l'information dans l'EGI et de sa présence dans l'EMI. Un commandant doit comprendre la puissance et le potentiel des médias, non seulement dans leur capacité à faire rapport sur une opération, mais également dans leur capacité à influencer leur auditoire cible en ce qui touche la *légitimité* de cette opération.

7. Le commandant doit anticiper la façon dont un adversaire peut tenter d'utiliser les médias pour parvenir à sa propre version de la supériorité de l'information. Le commandant doit également avoir les moyens de faire échec à ces tentatives de désinformation et de propagande pour atténuer les effets sur le moral de ses propres troupes. Par exemple, pendant la Guerre du Golfe, Saddam Hussein avait choisi comme cibles des missiles Scud des villes qui possédaient des organisations internationales de média d'information. L'intention était que la

couverture médiatique des pertes et dommages matériels aurait un effet négatif profond sur la population visée, et produirait une indication claire de la puissance militaire de l'Iraq. La coalition a fait échec à cette tentative de manipulation des médias en mettant à son tour l'accent sur les capacités des batteries de missiles Patriot.

8. On peut arguer que la présence de CNN à Baghdad s'insérait également dans le plan de supériorité de l'information de Saddam Hussein. Avec les reportages de CNN sur les dommages infligés à cette ville par les systèmes d'armes dits « intelligents » de la coalition, Saddam Hussein s'assurait que les auditoires partout dans le monde voyaient la douleur et la souffrance des civils irakiens et remettaient en question l'efficacité de la technologie utilisée contre le peuple irakien. Fait peut-être plus important encore, saddam Hussein a réussi à accroître la ferveur anti-américaine de son peuple à ses propres fins guerrières. Ces exemples illustrent comment les commandants tentent d'utiliser ou d'influencer les médias pour parvenir à leur objectif de supériorité de l'information.

SECTION 3
RÔLE DES AFFAIRES PUBLIQUES DANS LE SOUTIEN DES OPÉRATIONS D'INFORMATION

9. Les AP doivent être intégrées aux autres fonctions de combat parce qu'elles ont une incidence directe sur la conduite des opérations. Tout ce que l'Armée de terre fait pour accomplir sa mission se produit dans le cadre de l'EGI. Les opérations d'AP aident le commandant à comprendre et opérer dans le cadre de l'EGI en soutenant ses efforts pour satisfaire aux besoins d'information et aux attentes des auditoires internes et externes sans compromettre la mission.

10. L'objectif des AP est d'aider à assurer la supériorité de l'information en prenant l'initiative en ce qui a trait aux opérations médiatiques et en mettant en place des programmes qui :

a. protègent les soldats des effets de la propagande, de la désinformation et des rumeurs de l'ennemi, car des soldats bien informés sont des soldats efficaces;

b. favorisent la production de comptes rendus, ainsi que l'accès aux unités et aux soldats, ouverts et indépendants;

c. établissent les conditions menant à un climat de confiance dans l'Armée de terre;

d. fournissent une information équilibrée, juste et crédible sur les opérations de l'Armée de terre par la diffusion rapide d'une information complète, précise et opportune qui communique la version et les messages de l'Armée de terre grâce à un flux d'information complet, exact et opportun.

11. Il convient de noter que le rôle des AP est d'*informer*, et non d'*influencer*, ce qui, par définition, est le rôle des OPSPSY. S'il est possible que les auditoires cibles puissent être influencés par l'information qu'ils reçoivent, les distinctions clés résident dans l'*intention* visée par la fourniture de l'information et dans le fait que les OPSPSY doivent utiliser des moyens gouvernementaux ou militaires pour la production et la diffusion de leurs messages, et non les médias. Les OPSPSY peuvent utiliser l'information fournie par les médias pour renforcer ses messages, mais les AP ne peuvent pas servir à diffuser les messages des OPSPSY. La coordination entre les AP et les OPSPSY est toutefois essentielle pour assurer qu'il n'y a pas de contradiction ou de divergence.

12. Les commandants doivent comprendre que la *perception* d'une opération peut être aussi importante à son succès que l'*exécution* de cette opération. Les AP doivent être prises en compte et synchronisées tout au long du processus décisionnel, **car tout ce qui se produit au cours d'une opération a une dimension AP**.

13. Le personnel des AP soutient le commandant en faisant un suivi des perceptions du public, et en mettant au point et diffusant à l'intention des auditoires internes et externes des messages clairs et objectifs sur les opérations militaires, assurant ainsi que les opérations soient vues dans le contexte approprié et puissent être comprises.Le succès des opérations requiert une évaluation exacte de la situation des AP. L'évaluation AP consiste en une analyse continue de l'EGI et de son incidence possible sur l'opération. Elle fournit au commandant un examen exhaustif des facteurs d'AP critiques comme :

a. le nombre, les types et nationalités des représentants des médias d'information dans le théâtre;

b. l'identification de toute personnalité des médias d'information et leur organisation d'appartenance, de même que toute tendance ou tendance en matière d'information;

c. les besoins et limites des médias d'information;

d. les capacités de communications et de transport des médias d'information;

e. la perception que les auditoires internes et externes ont des opérations passées, courantes ou possibles.

14. Ces aspects doivent être pris en considération dans l'élaboration des stratégies et plans d'AP au soutien du concept global des opérations du commandant.

15. Le personnel des AP élaborera un plan qui non seulement appuie le commandant, mais également s'inscrit dans le cadre des objectifs d'AP au niveau national. Les répercussions possibles de la couverture médiatique des opérations (et de la réaction du public) doivent être évaluées, et le plan d'AP devra prendre en compte ces répercussions possibles. Ce faisant, toutefois, le principe de base des AP en ce qui touche la diffusion rapide d'une information complète, précise et opportune dans les limites des OPSEC ne doit pas être compromis.

16. Les stratégies et plans d'AP sont fondés sur les impératifs suivants :

a. **Pleine intégration des AP au processus de planification et de prise de décisions.** Pleinement intégrées au processus de planification à tous les niveaux, les AP fournissent au commandant les considérations essentielles qui doivent être prises en compte dans la visualisation de la zone d'opérations, l'évaluation de la situation et l'orientation de l'action militaire nécessaires à la victoire.

b. **Évaluation exacte de la situation des AP.** L'évaluation des AP est l'analyse continue de l'environnement de l'information, tant global que militaire, effectuée dans le but d'évaluer l'incidence possible de ce dernier sur l'opération. Elle fournit au commandant une analyse approfondie des facteurs d'AP critiques qui doivent être pris en considération dans la formulation et l'évaluation des plans d'action.

17. Les opérations d'AP comprennent quatre aspects :

a. **Planification.** La planification des AP fait partie intégrante du processus de prise de décisions et doit être incluse dès le début du niveau stratégique au niveau tactique. Les OAP doivent participer au processus à tous les niveaux afin de comprendre l'intention du

commandant supérieur et d'incorporer les activités d'AP qui appuient le concept des opérations de leur propre commandant et sont conformes à la ligne de conduite nationale. Les OAP visent à établir les conditions qui mènent à l'instauration d'un climat de confiance dans l'Armée de terre et l'opération en assurant la diffusion rapide d'une information complète, exacte et opportune qui communique la perspective de l'Armée de terre. Une telle diffusion de l'information aide à garantir que les représentants des médias comprennent les activités et événements qu'ils couvrent et en font un compte rendu équilibré et juste à nos auditoires tant externes qu'internes, contribue à réduire les contraintes qui limitent la gamme des possibilités du commandant et augmente la liberté d'action sans distraction de ce dernier. La planification inclut également la nécessité de conseiller le commandant et le personnel supérieur sur la gestion des problèmes et les communications en temps de crise concernant un large éventail de questions tant opérationnelles que non opérationnelles.

b. **Opérations avec les médias.** Les commandants et leur état-major doivent évaluer avec exactitude le niveau et l'intensité de l'intérêt des médias pour leur opération. Pour communiquer efficacement avec les médias d'information, leurs besoins doivent être anticipés à chacune des étapes d'une opération et ils doivent être satisfaits dans la mesure du possible, sans compromettre la sécurité des opérations ni le succès de la mission. Les opérations avec les médias incluent la prestation de conseils au commandant quant aux implications d'un compte rendu probable de son plan d'action par les médias. Les opérations avec les médias incluent également les éléments suivants :

(1) Facilitation de la couverture médiatique des opérations en anticipant et satisfaisant les besoins des médias. Ceci s'applique tout particulièrement aux médias qui accompagnent les troupes sur le terrain. Tous les médias requièrent une information exacte et opportune, ainsi que l'accès à des spécialistes en la matière. Les représentants des médias sur le théâtre des opérations peuvent toutefois avoir

des besoins additionnels comme le transport, l'hébergement et un soutien en matière de système d'information et de communications (SIC). Certains représentants des médias peuvent avoir besoin d'une formation rudimentaire en survie de manière à ne pas constituer un danger pour les troupes qu'ils couvrent ou pour eux-mêmes.

(2) Vérification de l'accréditation des médias et aide pour l'obtention de l'accréditation, selon les besoins.

(3) Discussion des règles de base touchant la couverture médiatique des opérations en cours et application de ces règles, selon les besoins.

(4) Établissement et maintien de Centres d'opérations des Affaires publiques (COAP).

c. **Communications internes.** Il est essentiel d'informer nos propres troupes tout au long des opérations, non seulement sur les questions liées aux opérations, mais également sur d'autres questions nationales (intérieures) et internationales. Il s'agit là d'une importante activité de maintien du moral et de contre-PSYOPS qui ne doit pas être oubliée dans la préparation et l'exécution des opérations. Ces activités d'information des troupes sont essentielles à l'élément de la puissance de combat qu'est le moral. Si un commandant n'informe pas les troupes, quelqu'un d'autre le fera en transmettant ses propres messages.

d. **Instruction en matière d'AP.** Étant donné le niveau d'intérêt des médias pour toutes les opérations militaires, il est nécessaire que les soldats apprennent à traiter efficacement avec les représentant des médias à l'intérieur comme à l'extérieur du champ de bataille. Le personnel des AP a un important rôle de soutien à cet égard. L'instruction en matière de sensibilisation aux médias doit être fournie à tous les soldats déployés et, si possible, à leur famille ainsi qu'au personnel resté sur place.

SECTION 4
CONSIDÉRATIONS EN MATIÈRE DE PLANIFICATION DES AFFAIRES PUBLIQUES

18. Le plan d'AP doit être entièrement coordonné avec le plan opérationnel, et devient habituellement une annexe de ce dernier. Pendant la mise au point d'un plan d'AP, les facteurs qui suivent sont pris en considération :

a. **Accès des représentant des médias.** Pour comprendre la situation dans son ensemble, les journalistes doivent avoir accès aux soldats, unités et formations déployés. L'accès des médias doit être planifié et facilité dans toute la mesure du possible, de manière à garantir que les médias d'information ne compromettront pas la mission et ne mettront pas en danger les soldats qu'ils couvrent. Les forces déployées doivent en venir à s'attendre à la présence des médias dans leur secteur, et doivent être préparées à aider les médias d'information à avoir accès aux secteurs accessibles seulement par des moyens militaires. L'absence d'un plan d'accès des médias résultera en une couverture médiatique non planifiée et risque, en bout de ligne, de compromettre la mission ou la compréhension de l'opération par les médias et le public.

b. **Sécurité.** La sécurité des opérations (OPSEC) est une des principales préoccupations des planificateurs de la mission et un élément fondamental de la planification en matière d'AP. Les préoccupations du commandant en ce qui touche la sécurité doivent être prises en compte dans la planification du moment et de l'étendue de la visite que les médias d'information seront autorisés à faire, et de ce qui sera dit. L'accès des médias doit être planifié à l'avance et toute restriction appropriée doit être appliquée de façon uniforme par la voie hiérarchique, afin de ne pas compromettre la crédibilité de cette dernière et du personnel des AP. Les représentants des médias doivent être informés le plus tôt possible des lignes directrices applicables en matière de reportage. Celles-ci seront énoncées dans le cadre du plan opérationnel d'ensemble. Le non-respect de ces lignes directrices par les représentants des médias pourrait entraîner la suspension des privilèges de visite.

Les impératifs de sécurité à la source doivent régir toutes les conversations avec les médias et il convient d'insister sur le fait qu'il n'y a rien de moins confidentiel que des propos tenus en toute confidence.

c. **Soutien des médias.** La planification pour faire face à l'imprévu devrait inclure les ressources en matériel, en transport et en communications nécessaires pour aider les médias d'information accrédités à recueillir l'information et à transmettre leur reportage. Les arrangements relatifs à l'utilisation de ressources de SIC doivent être fondés sur la disponibilité de ces ressources sur une base de non interférence, et être autorisés seulement dans les cas où des services commerciaux ne sont pas disponibles.

d. **Information interne.** Les besoins de l'auditoire interne doivent être pris en considération dans le processus de planification des AP. Il est d'une importance critique que cet auditoire ait une bonne compréhension, laquelle repose sur la communication d'une information exacte et opportune en provenance des unités et formations déployées. Les médias d'information sont une importante voie de transmission de cette information, mais ne peuvent pas servir à communiquer des messages de la part des forces amies à l'auditoire interne. D'autres moyens de transmission de l'information, comme des organes de nouvelles internes et Internet, doivent être envisagés et font partie intégrante du plan d'AP pour l'opération.

SECTION 5
COMMANDEMENT ET CONTRÔLE DES AFFAIRES PUBLIQUES

19. Les organisations d'AP déployées doivent être aptes à s'acquitter de la mission, modulaires, souples, agiles, suffisamment équipées et positionnées stratégiquement de manière à soutenir le commandant dans la lutte en vue de la supériorité de l'information.

20. Une fois l'opération amorcée, la priorité des efforts du personnel d'AP consiste à établir un COAP identifiable pour soutenir le commandant en maintenant en puissance les efforts des représentants des médias d'information qui accompagnent les unités et en communiquant

avec ceux qui ne sont pas sur place. En s'appuyant sur les principes de modularité et de flexibilité, le COAP doit accroître sa capacité parallèlement à celle de la force déployée. Être apte à s'acquitter de la mission signifie que le personnel des AP doit être capable de répondre à la demande de contribution des AP au plan opérationnel et aux communications internes faite par le commandant, ainsi qu'aux exigences croissantes des médias d'information qui couvrent l'opération. Des plans doivent être en place pour permettre l'expansion de l'organisation des AP selon les besoins. Cette capacité contribuera à garantir qu'une infrastructure crédible de relations avec les médias est en place, et réduira le risque que des représentants des médias mal informés et non coopératifs nuisent à l'opération. Le déploiement de l'organisation des AP doit parvenir au difficile équilibre entre la disponibilité requise pour mener des activités de planification et assurer le fonctionnement du COAP. Ce dernier doit être l'endroit où les médias seront réunis, ce qui est le plus souvent le dernier endroit où le commandant voudra installer son QG.

21. L'Armée de terre opérera souvent dans le cadre d'équipes interarmées ou combinées. Dans les opérations interarmées où la force principale est fournie par l'Armée de terre, l'OAP supérieur de l'Armée de terre agira normalement à titre d'OAP en chef pour l'opération. Il est entendu que les QG des différentes armées peuvent avoir leur propre personnel d'AP, mais ce personnel travaillera principalement aux activités de communication internes. Le contact avec les représentants des médias et les organisations externes à leur commandement sera coordonné par le COAP de l'armée principale. Dans les situations où d'autres éléments ou agences assurent la direction des AP, l'Armée de terre fournira du personnel d'AP pour aider à l'établissement et au fonctionnement d'un COAP interarmées ou multinational. Une coordination et une liaison continues entre les éléments d'AP au sein d'un COAP interarmées ou multinational sont d'une importance critique pour garantir que les buts stratégiques de l'opération, le rôle de l'Armée de terre dans l'opération, et les problèmes et questions de sécurité sont clairement compris.

22. La fonction AP est une composante de soutien essentielle et séparée des OI. L'OAP supérieur est un conseiller spécialiste du commandant, et est responsable de la coordination des opérations avec les médias. La planification des AP, la gestion des problèmes et des communications en temps de crise (les besoins d'instruction en matière de sensibilisation aux médias seront coordonnés par l'état-major général) pour le théâtre d'opérations. L'OAP supérieur s'assure également que la ligne de conduite nationale et les stratégies d'AP sont incorporées aux processus de planification du commandant. Le soutien administratif pour

le théâtre d'opérations est tributaire de la mission, mais est assuré par les quartiers généraux appuyés.

23. Comme il est souligné dans la B-GL-300-003/FP-000, *Commandement,* un commandant doit posséder, pour être efficace, un large éventail de qualités et de compétences, en plus du savoir-faire strictement militaire. Ces qualités et compétences incluent une compréhension de la politique nationale et internationale, de l'économie politique mondiale, des affaires étrangères, de la gestion et de la planification d'entreprise, et du droit international des conflits armés. Différents commandants approcheront ces défis de différentes façons. La principale force de l'OAP est sa capacité à évaluer comment le commandant veut relever les défis d'AP liés au commandement. Le concept des opérations d'AP du commandant doit être clairement compris par l'OAP, et les stratégies et plans d'AP dans le théâtre doivent prendre cet impératif en considération. Certains commandants peuvent préférer conserver le rôle de porte-parole officiel de leur formation, tandis que d'autres auront une approche plus décentralisée et délégueront à des spécialistes en la matière la tâche de parler sur des questions de fond. Le personnel d'AP soutient la chaîne de commandement en s'assurant que les porte-parole désignés sont bien préparés à s'entretenir avec les médias sur ces questions.

CHAPITRE 8
COOPÉRATION CIVILO-MILITAIRE

L'importance de la dimension civile du champ de bataille moderne ne diminuera pas, elle ne fera que s'accroître. Les chefs et commandants supérieurs ne peuvent plus reléguer la planification des Opérations civilo-militaires (OCM) au statut d'activité accessoire. Les OCM devraient être considérées comme étant tout aussi importantes que les autres fonctions de combat.

Major T.E. Howie, Armée des É.-U.

SECTION 1
INTRODUCTION ET DÉFINITIONS

1. La coopération civilo-militaire (COCIM) a toujours constitué une composante des opérations militaires. La COCIM est un élément intégral des Opérations d'information (OI), car elle fournit de l'information vitale au commandant sur le gouvernement civil et la population, lesquels ont une incidence sur ses opérations. La COCIM se définit comme étant « *en temps de paix, de conflit et de guerre, l'ensemble des mesures entreprises conjointement par les commandants et les autorités nationales civiles, militaires et para-militaires, qui concernent la relation entre les Forces canadiennes, les gouvernements nationaux et les populations civiles dans une région où les forces militaires canadiennes sont déployées ou prévoient être déployées, soutenues ou utilisées. Ces mesures incluent également la coopération et la coordination des activités entreprises conjointement par les commandants et les agences, organisations et autorités non-gouvernementales ou internationales* »[15]. La COCIM est une responsabilité des commandants.

2. Dans le passé, la COCIM était axée sur le contrôle militaire de la population civile dans la zone d'opérations et visait à garantir que les civils ne nuiraient pas aux opérations militaires. Cela est particulièrement vrai en temps de crise et de guerre. En guise d'exemple, la directive qui suit avait été émise le 1er mai 1944 par le Quartier général suprême du

---

[15] B-GG-005-004/AF-023, *Cooperation civilo-militaire en temps de paix, d'urgence, de crise et de guerre*

Corps expéditionnaire allié : « Une responsabilité majeure de chaque commandant est de s'assurer que les conditions qui prévalent dans la population civile ne gênent pas les opérations contre l'ennemi, mais les favorisent dans toute la mesure du possible »[16].

3. Par contraste avec la conduite de la guerre, les opérations autres que la guerre ont changé la façon dont l'Armée de terre voit la COCIM. Des missions militaires entières sont maintenant basées sur la COCIM comme moyen d'atteinte de l'objectif politique. L'aide humanitaire, l'assistance au Haut Commissariat des Nations Unies pour les réfugiés (HCR) et la surveillance des élections ne sont que quelques exemples de la façon dont l'armée a été utilisée au soutien des civils en vue de l'atteinte d'un objectif politique. La COCIM est menée par les forces militaires dans l'éventail des situations de conflit possibles. En temps de paix, l'Armée de terre mène généralement des opérations qui appuient la population civile et les gouvernements. Lorsque la situation se détériore/dégénère, l'accent sur la COCIM passe du soutien des organismes civils à des activités visant à garantir que les opérations militaires peuvent se poursuivre dans la partie opérations de guerre du spectre des conflits et du continuum des opérations. Ceci est illustré à la Figure 8-1-1.

---

[16] Standard Policy and Procedures for Combined Civil Affairs Opérations in North West Europe, 1 mai 1944

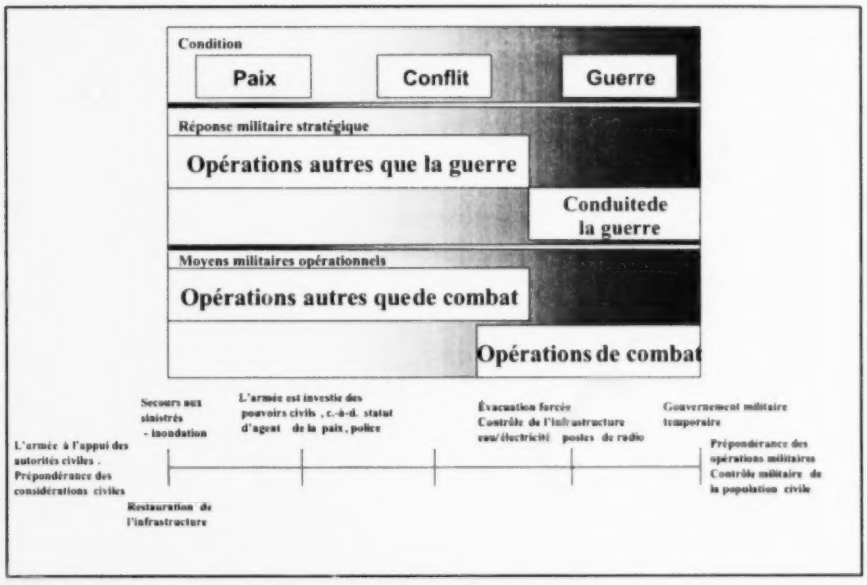

Figure 8-1-1 : COCIM et le spectre des conflits

4. L'information recueillie au moyen de la COCIM est d'une importance critique pour le commandant. La plupart des activités militaires concernant les civils postulent l'obtention d'information ou l'influence des perceptions des civils dans le but d'obtenir leur coopération, avec l'usage de la force en tout dernier recours. Même en temps de guerre dans un territoire hostile, les activités de COCIM tenteront de rallier le soutien et la coopération de la population civile afin que les opérations militaires ne soient pas compromises.

SECTION 2
OBJECTIFS DE L'ARMÉE DE TERRE EN MATIÈRE DE COOPÉRATION CIVILO-MILITAIRE

5. Le principal objectif de la COCIM est d'assurer la coopération nécessaire entre les autorités civiles et le commandant afin que ce dernier puisse réaliser son objectif. Dans les opérations intérieures et internationales, les objectifs de COCIM des opérations de l'Armée de terre sont fondamentalement conformes aux objectifs énoncés dans le manuel des Forces canadiennes :

a. soutenir les intérêts nationaux canadiens;

b. remplir les obligations imposées par le droit national (Loi sur la défense nationale, lois intérieures) et le droit international (droit des conflits armés, droit

international en matière de droits de la personne), ainsi que par toute entente ou convention entre les autorités nationales ou parties à l'accord;

c. conseiller, assister ou renforcer des gouvernements étrangers conformément à la politique nationale et aux exigences opérationnelles;

d. soutenir la mission du commandant;

e. soutenir des objectifs politico-militaires canadiens spécifiques dans le théâtre ou la zone d'opérations;

f. assister le commandant au soutien de l'administration civile;

g. faciliter la mission du commandant en minimisant une interférence de la population locale au cours de la phase militaire d'une opération, et en obtenant le soutien des civils pour la phase civile et les tâches connexes;

h. aider le commandant à s'acquitter d'obligations légales et morales vis-à-vis de la population locale;

i. déterminer et coordonner l'utilisation des ressources locales, des installations et du niveau de soutien requis en vue du rétablissement des gouvernements locaux;

j. aider le commandant, en fournissant les ressources nécessaires à la satisfaction des besoins civils essentiels, en évitant les dommages à la propriété civile et aux ressources utilisables, en minimisant les pertes de vie humaine et la souffrance humaine, en assumant la présence d'une organisation de COCIM;

k. appuyer de la façon requise les organismes internationaux, les organisations non gouvernementales (ONG), les Nations Unies et l'Organisation pour la sécurité et la coopération en Europe (OSCE), de même que l'OTAN ou les agences civiles nationales, dans tous les types de coopération civilo-militaire, et ce, à un niveau spécifié par le gouvernement ou le QGDN;

l. aider les autorités locales à créer, rétablir et maintenir la loi et l'ordre public.

6. Le commandant et l'état-major doivent être très spécifiques dans leurs attentes des fonctions qui doivent être remplies dans le cadre de la

COCIM. La figure 8-2-2montre l'étendue et les délimitations des types d'opérations auxquels les Forces terrestres peuvent être appelées à participer sous les auspices de l'OTAN ou de l'ONU.

Figure 8-2-2 : L'environnement opérationnel

SECTION 3
TYPES DE COOPÉRATION CIVILO-MILITAIRE

7. Il existe deux types de COCIM : les opérations civilo-militaires et le soutien à l'administration civile. La figure 8-3 montre les différentes composantes de la COCIM et leurs interactions au soutien d'une opération militaire.

8. Les deux types de COCIM se subdivisent en trois domaines fonctionnels :

a. **Négociation d'ententes de coordination et de soutien.** Ces activités devraient être planifiées et négociées par une autorité unique désignée présente dans le théâtre, au cours des premières étapes de la planification de campagne, et porter sur toutes les phases de l'opération.

b. **Coordination du soutien civilo-militaire (SCM).** Le SCM englobe toutes les activités qui nécessitent une interaction, une coordination ou une coopération civilo-militaires.

c. **Coordination avec la planification civile d'urgence (PCU).** Il s'agit d'une responsabilité nationale. Des considérations touchant les environnements tant intérieur qu'international sont expliquées dans le manuel sur la COCIM des Forces canadiennes.

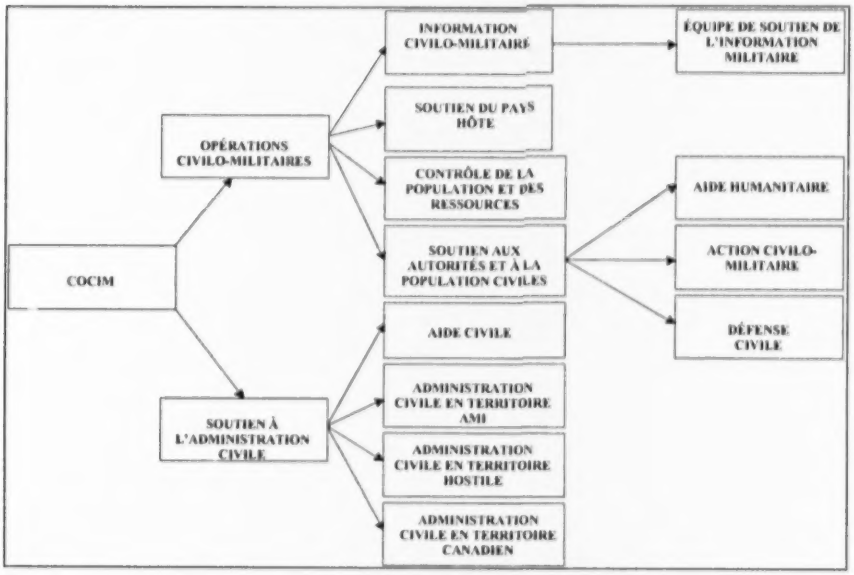

Figure 8-3-3 : Types de coopération civilo-militaire

SECTION 4
LIENS ENTRE LA COOPÉRATION CIVILO-MILITAIRE, LES OPÉRATIONS PSYCHOLOGIQUES ET LES AFFAIRES PUBLIQUES

9. L'information est le point commun entre la COCIM, les Opérations psychologiques (OPSPSY) et les Affaires publiques. La COCIM utilise l'information pour informer le public du théâtre d'opérations sur les programmes d'aide et les projets de reconstruction dans leur région. Les AP utilisent l'information pour gérer les problèmes et informer les troupes, les Canadiens, et la population de la zone d'opérations de ses activités dans la région. Les OPSPSY utilisent l'information pour tenter de modifier les perceptions, opinions, attitudes,

comportements et convictions d'une population de manière à obtenir son appui aux tâches civiles, ainsi qu'aux activités militaires et civiles, dans le but d'améliorer l'unité des efforts et de mener à un engagement des chefs politiques et militaires à créer des conditions politiques, sociales, économiques et contextuelles en vue d'une paix structurelle et durable.

10. La COCIM est une fonction que les Forces canadienne et l'Armée de terre ont assumée sous d'autres noms, dans des opérations intérieures, mais principalement sous la forme d'activités « spéciales » dans le cadre d'opérations internationales. Ces activités spéciales de COCIM n'étaient toutefois pas intégrées au plan du commandant.

SECTION 5
SOURCES D'INFORMATION

11. Les sources d'information varient selon le domaine d'intérêt de la COCIM. Les sources liées au soutien des forces touchent principalement la logistique, les autres pays et les chefs militaires locaux. Les sources liées au contexte civil touchent les structures administratives, les conditions de vie, l'économie, les actions humanitaires et la population. Les principales sources d'information sont les suivantes :

a. **Interprètes.** Les interprètes locaux sont une des meilleures sources d'information locale. Il est nécessaire de faire preuve de prudence, car ils peuvent poursuivre des buts personnels ou ceux d'une faction. Ils ont une connaissance intime de la politique, de la société et des coutumes locales. Ils sauront immédiatement à qui s'adresser, et seront à même de percevoir des situations anormales. Ils sont reconnus par la population locale comme étant un des leurs, et on leur répond plus spontanément qu'on le ferait à tout membre de la COCIM. Les interprètes sont un élément essentiel de l'équipe de COCIM. Leur valeur est beaucoup plus grande que leur simple capacité de parler la langue locale. Leur appartenance à l'équipe de COCIM crée toutefois un certain dualisme. Ils essaient spontanément de satisfaire aux exigences de leur poste tout en conservant leurs convictions et idéaux personnels. On doit y faire appel avec circonspection et leur loyauté doit être vérifiée périodiquement. L'utilisation d'interprètes locaux devrait s'accompagner de l'utilisation d'un interprète militaire dans les cas où la question est sensible ou critique au succès de la mission.

b. **Organisations et agences.** Les agences nationales et internationales, les gouvernements étrangers, les organisations bénévoles privées (OBP), les ONG, et diverses autres organisations sont d'excellentes sources d'information et de soutien de la COCIM. Ces organisations ont habituellement été présentes dans le pays beaucoup plus longtemps que notre force et possèdent, sur les activités locales, une perspective « du dehors » qui vaut d'être analysée. Les contacts du personnel de COCIM avec ces entités se font de manière officieuse et sans aucune des formalités militaires. La quantité d'interaction ou de protection, et donc de contact, avec une organisation donnée est déterminée par la charte de l'organisation en question. Certaines sont plus ouvertes que d'autres à l'aide militaire.

c. **Réfugiés.** De manière générale, la fragilité psychologique des réfugiés les amène à être très éloquents sur les événements et incidents personnels de leur périple. Leur interprétation des événements est toutefois déformée par le choc ou traumatisme qu'ils ont vécu. Toute information obtenue de réfugiés devrait être transmise au renseignement pour traitement.

d. **Factions politiques, religieuses ou ethniques.** La direction des différentes factions est le point de contact habituel du personnel de COCIM. Il est nécessaire d'établir un contact avec chacune des factions pour maintenir une impartialité objective. Les groupes d'intérêt spéciaux ont toutefois tendance à vouloir expliquer leur position « particulière » et il peut être difficile d'établir les faits. Néanmoins, il est souhaitable d'établir un contact ou d'avoir une connaissance de ces factions. Mais, encore une fois, toute information obtenue de ces factions devrait être couramment transmise au renseignement.

e. **Population.** Il est profitable de parler aux gens ordinaires. On peut ce faisant jauger le climat local et l'information obtenue à des niveaux supérieurs. Une compréhension populaire du mode de vie, des préoccupations et inquiétudes locales est la première étape dans l'analyse tant des sources d'information que

des résultats des actions de COCIM, et permet aux cellules opérationnelles d'anticiper les événements possibles résultant de l'évolution de la situation actuelle.

SECTION 6
COCIM ET INFORMATION

12. La première mission de la COCIM est de soutenir les opérations. Leur capacité à recueillir et transmettre de l'information doit être évaluée par rapport à la nécessité d'accomplir la mission première. L'information à destination et en provenance de la COCIM doit suivre une voie reconnue, au sein des forces, et être intégrée au processus de planification normal.

a. **Détermination du besoin.** Même si la collecte d'information est un réflexe élémentaire pour le personnel de COCIM, les besoins spécifiques doivent être définis par l'entremise de la procédure de combat. Le Centre d'opérations civilo-militaires (COCM) sert de principal point de réception de l'information recueillie par la COCIM.

b. **Planification.** Le COCM est responsable de l'élaboration du plan de collecte de la COCIM. Ce plan inclut les directives du G5, l'intention et les orientations du commandant, et la contribution du renseignement et du G3. Les objectifs d'information peuvent ne pas être facilement atteignables parce que la mission de la COCIM est l'objectif premier. Les besoins essentiels du commandant en information (BECI) doivent être utilisés pour orienter la participation de la COCIM au processus de collecte d'information.

c. **Collecte d'information.** Le COCM assigne les demandes d'information accompagnées des contraintes canadiennes s'y rapportant, et attend les résultats. Le personnel de COCIM fait rapport à l'officier des opérations du COCM. Cet officier étudie et compare les rapports et les transmet à la cellule du renseignement. Cette dernière transmet également un rapport sur la demande d'information aux bureaux concernés. Comme nous l'avons mentionné précédemment, l'officier des opérations du COCM doit être sensibilisé au risque

d'actions de désinformation possibles contre les Forces canadiennes et faire preuve de vigilance.

d. **Interactions**. Le personnel de la COCIM ne doit pas oublier qu'il est une ressource d'information au soutien des opérations. Une liaison constante doit être établie avec la cellule des opérations, ainsi qu'un lien technique avec la cellule du renseignement et l'OAP. En même temps, des vérifications doivent être effectuées périodiquement auprès d'autres bureaux pour garantir que les communications sont transmises.

e. **Évaluation périodique de la COCIM.** Une évaluation à jour de la COCIM doit être transmise périodiquement à l'état-major général sur la situation actuelle. En cas de changements importants dans l'évaluation de la COCIM, le G5 doit faire rapport au chef d'état-major et faire une nouvelle proposition. Dans les Opérations d'information, le G5 n'est qu'une ressource au soutien des opérations.

SECTION 7
LIMITATIONS / ACTIVITÉS NON AUTORISÉES

13. La COCIM, les PSYOPS et les AP doivent être coordonnées et gérées avec soin de manière qu'elles n'outrepassent pas la portée de leur champ d'action; elles risquent autrement de se compromettre elles-mêmes. Essentiellement, aucune de ces organisations ne devrait mener une campagne qui nuirait aux opérations des deux autres fonctions. La coordination et la synchronisation des activités de ces organisations sont donc capitales à la réalisation de la mission du commandant.

14. Dans la plupart des cas, le personnel de la COCIM peut disposer de la liberté de mouvement nécessaire à la réalisation de sa mission. Il y a cependant des périodes où le niveau des hostilités empêche le personnel de COCIM d'être aussi actif qu'il le devrait. Le personnel peut faire face à des risques élevés et bénéficier d'une protection très réduite pendant l'accomplissement de sa mission. Le cas échéant, l'état-major pourra juger opportun de réviser le plan de COCIM ou certaines de ses priorités internes.

ANNEXE A
SOUTIEN MUTUEL DES ÉLÉMENTS DES OPÉRATIONS D'INFORMATION OFFENSIVES ET DÉFENSIVES

	SECOP	CI	DÉCEPTION MILITAIRE	OPSPSY	CONTRE-OPSPSY	GE	ARO	OI SPÉCIALES	DESTRUCTION MATÉRIELLE
SECOP		L'évaluation de CI détermine les paramètres et risques en matière de SECOP. Les activités de CI soutiennent SECOP.	Cache des faits observables conflictuels. Dégrade l'information sur la situation générale pour améliorer l'effet des opérations de déception.	Cache de l'information conflictuelle. Dégrade la situation générale pour améliorer l'effet des OPSPSY.	Détermine les risques de OPSPSY d'un adversaire qui doivent être contrés.	Cache les unités et systèmes de GE pour empêcher l'accès à l'information quant à l'importance des capacités de MSGE/CME.	Cache le potentiel d'ARO ami.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Cache les systèmes spécialisés pour permettre aux OI offensives d'empêcher l'accès à l'information quant à l'importance de leurs capacités.
CI	Les mesures de SECOP compensent les points vulnérables repérés par la CI.		Aide à déterminer la vulnérabilité de l'adversaire aux efforts de déception.	Cache nos capacités de OPSPSY.	S/O	Confirme les succès de CI.	Fournit un suivi sur le succès des ARO.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Fournit une forme d'EDC.
DÉCEPTION MILITAIRE	Amène l'adversaire à ne pas recueillir d'information sur les activités des unités protégées. Amène l'adversaire à sous-estimer les mesures de SECOP amies. Fournit de l'information pour combler les « trous » créés par les mesures de SECOP amies.	Désoriente les capacités ISTAR de l'adversaire.		Fournit de l'information compatible avec le thème des OPSPSY. Renforce le thème des OPSPSY au moyen d'activités de déception.	Amène l'adversaire à croire que les OPSPSY ne seront pas efficaces.	Amène l'adversaire à : Sous-estimer les capacités de MSGE/CME amies. Défendre les mauvais systèmes de commandement et de contrôle contre les MSGE/CME amies.	Rend l'adversaire plus sujet aux effets des ARO.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Amène l'adversaire à : Sous-estimer le potentiel de destruction des OI offensives amies. Défendre le mauvais élément/système de commandement et de contrôle contre une destruction ISTAR amie.
OPSPSY	Protègent l'information sur les opérations autres que la guerre. Créent des perceptions adaptées aux activités de SECOP.	Aident à déterminer les objectifs pour les OPSPSY.	Créent des perceptions et attitudes qui peuvent être exploitées par la déception militaire. Intègrent les actions des OPSPSY et des efforts de déception.		Aide à mettre en place les conditions propices à l'efficacité des OPSPSY.	Utilisent les ressources de OPSPSY pour diffuser des produits sur les fréquences de l'adversaire. Mettent au point des messages pour diffusion sur d'autres ressources de GE.	Amènent l'adversaire à croire que nos capacités d'ARO sont beaucoup plus grandes qu'elles le sont en réalité.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Amènent la population à fuir les régions désignées comme objectif. Réduisent la limitation du dommage collatéral en cas de destruction de l'infrastructure de commandement et de contrôle de l'adversaire.
CONTRE-OPSPSY	Améliorent la position en matière de SECOP.	Déterminent et neutralisent les agents d'influence (tant amis qu'adversaires)	Déterminent l'utilisation de OPSPSY par l'adversaire à des fins de déception.	Contrent les effets des OPSPSY de l'adversaire.		Aident à déterminer le succès des CME.	Réduisent l'utilisation des OPSPSY par l'adversaire au moyen d'ARO.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Réduisent les effets des OPSPSY de l'adversaire sur les unités.

	SECOP	CI	DÉCEPTION MILITAIRE	OPSPSY	CONTRE-OPSPSY	GE	ARO	OI SPÉCIALES	DESTRUCTION MATÉRIELLE
GE	Dégrade les ressources EM ISTAR de l'adversaire qui visent les unités et activités protégées. Couvre les brèches de de courte durée en matière de SECOP.	Aide à déterminer la capacité de l'adversaire à mettre en œuvre des MSGE/CME.	Mène des activités de déception au moyen de MSGE/CME. Dégrade la capacité de l'adversaire à voir, signaler et traiter des faits observables conflictuels. Empêche l'accès des décideurs à l'information à des moments critiques pour améliorer les effets des activités de déception.	Dégrade la capacité de l'adversaire à voir, signaler et traiter de l'information conflictuelle. Empêche l'accès d'un auditoire cible à l'information conflictuelle.	Aide à déterminer le succès du programme de contre-OPSPSY.		Utilisée comme moyen d'ARO.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Effectue l'acquisition d'objectif pour les OI offensives au moyen de MSGE. Détruit ou perturbe les ressources vulnérables qui utilisent des MSGE au moyen de CME.
ARO	Convainc l'adversaire que la position en matière de SECOP est meilleure qu'elle ne l'est.	Attaque les capacité ISTAR de l'adversaire.	Utilise l'ARO dans le cadre des activités de déception.	Réduit la confiance d'un adversaire en ses propres réseaux d'ordinateurs.	Attaque les moyens utilisés par les OPSPSY de l'adversaire.	S/O		Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	Utilisée en conjonction avec d'autres activités de destruction.
OI SPÉCIALES	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.	Aident ou soutiennent d'autres éléments en fonction des besoins.		Aident ou soutiennent d'autres éléments en fonction des besoins.
DESTRUCTION MATÉRIELLE	Empêche une action ou dégrade les ressources ISTAR de l'adversaire contre les unités et activités protégées.	Identifie et neutralise les saboteurs.	Conduit des attaques à des fins de déception. Dégrade les capacités de l'adversaire à voir, signaler et traiter des faits observables conflictuels. Isole les décideurs de l'information à des moments critiques pour améliorer les effets des activités de déception.	Dégrade la capacité de l'adversaire à voir, signaler et traiter de l'information conflictuelle. Dégrade la capacité d'un adversaire à brouiller les émissions de OPSPSY. Empêche l'accès d'un auditoire cible à l'information conflictuelle.	Dégrade le potentiel de OPSPSY d'un adversaire.	Réduit le nombre d'objectifs de CME amis protégés par les OI défensives en sélectionnant et coordonnant la destruction de l'infrastructure de commandement et de contrôle de l'adversaire. Détruit des systèmes électroniques sélectionnés pour forcer l'adversaire à utiliser des systèmes vulnérables aux MSGE/CME amies.	Dégrade la capacité d'un adversaire à mener une ARO.	Selon la nature des OIS. Tout élément peut être utilisé au soutien des OIS.	